# POLISI KESELAMATAN SIBER NEGERI MELAKA

VERSI 1.0

## SEJARAH DOKUMEN POLISI KESELAMATAN SIBER NEGERI MELAKA

| TARIKH | VERSI | KELULUSAN | TARIKH KUATKUASA |
|---|---|---|---|
| April 2026 | 1.0 | Mesyuarat Jawatankuasa Pemandu ICT Bil 1/2026 | 1 April 2026 |

# ISI KANDUNGAN

**PENGENALAN** ..... **7**
**OBJEKTIF** ..... **7**
**PERNYATAAN DASAR** ..... **8**
**SKOP** ..... **9**
**PRINSIP-PRINSIP POLISI KESELAMATAN SIBER NEGERI MELAKA** ..... **10**
**PENILAIAN RISIKO KESELAMATAN ICT** ..... **12**
**BIDANG 5: KAWALAN ORGANISASI** ..... **13**
**5.1: Polisi Keselamatan Maklumat** ..... **13**
5.1.1: Objektif Dasar ..... 13
5.1.2: Pengesahan Dan Pelaksanaan Dasar ..... 14
5.1.3: Penyebaran Dan Perakuan Dasar ..... 14
5.1.4: Penyelenggaraan Dasar ..... 14
5.1.5: Pengecualian Dasar ..... 15
**5.2: Tanggungjawab dan Peranan dalam Keselamatan Maklumat** ..... **15**
5.2.1: Setiausaha Kerajaan Negeri (SUK) ..... 15
5.2.2: Ketua Pegawai Digital (CDO) ..... 16
5.2.3: Pegawai Keselamatan ICT (ICTSO) ..... 16
5.2.4: Jawatankuasa Pemandu ICT (JPICT) Negeri Melaka ..... 17
5.2.5: Cyber Security Incident Response Team (CSIRT) ..... 18
5.2.6: Pengguna ..... 20
5.2.7: Juru Audit Dalaman ..... 21
5.2.8: Pihak Ketiga ..... 21
**5.3: Pengasingan Tugas** ..... **22**
5.3.1: Pentadbir Sistem Aplikasi ..... 22
5.3.2: Pentadbir Rangkaian ..... 23
5.3.3: Pentadbir Laman Web ..... 24
5.3.4: Pentadbir E-mel ..... 25
5.3.5: Pentadbir Active Directory (AD) / Domain Controller ..... 27
5.3.6: Pentadbir Pangkalan Data ..... 28
5.3.7: Pentadbir *Backup* Data ..... 29
5.3.8: Pegawai Aset ICT dan Pentadbir Teknikal ..... 30
5.3.9: Pentadbir Pusat Data ..... 31
**5.4: Tanggungjawab Pengurusan** ..... **32**
5.4.1: Pengurusan Tertinggi ..... 32
**5.5: Hubungan Dengan Pihak Berkuasa** ..... **33**
**5.6: Hubungan Dengan Pihak Berkepentingan** ..... **33**

**5.7: Perisikan Ancaman** ..... **33**
**5.8: Keselamatan Maklumat di Dalam Pengurusan Projek** ..... **34**
**5.9: Maklumat Inventori & Aset-aset Lain Yang Berkaitan** ..... **35**
**5.10: Kebenaran Penggunaan Maklumat Dan Aset Berkaitan** ..... **36**
**5.11: Pemulangan Aset** ..... **37**
**5.12: Pengelasan dan Pengendalian Maklumat** ..... **38**
5.12.1: Pengelasan Maklumat ..... 38
5.12.2: Pengendalian Maklumat ..... 38
**5.13: Pelabelan Maklumat** ..... **39**
**5.14: Pemindahan Maklumat (*Information Transfer*)** ..... **40**
5.14.1: Pemindahan Maklumat ..... 40
5.14.2: Penggunaan E-mel ..... 40
**5.15: Kawalan Capaian** ..... **43**
5.15.1: Keperluan Kawalan Capaian ..... 43
5.15.2: Kawalan Capaian Sistem Pengoperasian ..... 46
5.15.3: Kawalan Capaian Aplikasi Dan Maklumat ..... 47
**5.16: Pengurusan Identiti** ..... **48**
5.16.1: Akaun Pengguna ..... 48
**5.17: Maklumat Pengesahan** ..... **50**
5.17.1: Pengurusan Katalaluan ..... 50
**5.18: Hak Capaian** ..... **51**
5.18.1: Semakan Hak Capaian Pengguna ..... 51
5.18.2: Pembatalan atau Kemas kini Hak Capaian ..... 51
**5.19: Hubungan Keselamatan Maklumat Dengan Pembekal** ..... **52**
**5.20: Perjanjian Keselamatan Maklumat Dengan Pembekal** ..... **53**
**5.21: Pengurusan Keselamatan Maklumat Dalam Rantaian Komunikasi** ..... **54**
**Maklumat ICT** ..... **54**
**5.22: Pemantauan, Semakan Dan Perubahan Pengurusan Perkhidmatan** ..... **54**
**Pembekal** ..... **54**
**5.23: Keselamatan Maklumat Bagi Penggunaan Perkhidmatan Awan** ..... **55**
**5.24: Perancangan, Penyediaan Dan Pengurusan Insiden Keselamatan** ..... **56**
**Maklumat** ..... **56**
**5.25: Penilaian Dan Keputusan Peristiwa Keselamatan Maklumat** ..... **57**
**5.26: Maklumbalas Insiden Keselamatan Maklumat** ..... **58**
**5.27: Pembelajaran Daripada Insiden Keselamatan Maklumat** ..... **59**
**5.28: Pengumpulan Bukti** ..... **59**
**5.29: Keselamatan Maklumat Semasa Gangguan** ..... **60**
5.29.1: Pelan Kesinambungan Perkhidmatan ..... 60
5.29.2: *Backup* dan *Restore* ..... 60

**5.30: Ketersediaan ICT Untuk Kesinambungan Perkhidmatan ..... 61**
**5.31: Pematuhan Terhadap Keperluan Perundangan, pekeliling, Peraturan Dan..... 63**
**Perjanjian Kontrak ..... 63**
**5.32: Hak Harta Intelek ..... 64**
**5.33: Perlindungan Rekod ..... 64**
**5.34: Privasi dan Perlindungan Maklumat Pengenalan Peribadi ..... 64**
**5.35: Semakan Semula Keselamatan Maklumat ..... 65**
**5.36: Pematuhan Polisi, Peraturan Dan Piawaian Keselamatan Maklumat ..... 65**
**5.37: Prosedur Operasi Yang Didokumen ..... 65**
**BIDANG 6 – KAWALAN MANUSIA ..... 67**
**6.1: Saringan ..... 67**
**6.2: Terma Dan Syarat Pekerjaan ..... 68**
**6.3: Kesedaran Keselamatan Maklumat, Pendidikan Dan Latihan ..... 69**
**6.4: Proses Tindakan Tatatertib ..... 70**
**6.5: Tanggungjawab Selepas Penamatan Atau Perubahan Pekerjaan ..... 71**
**6.6: Kerahsiaan atau Perjanjian *Non-Disclosure* ..... 73**
**6.7: Bekerja Luar Pejabat ..... 73**
**6.8: Pelaporan Keselamatan Maklumat ..... 75**
**BIDANG 7 – KAWALAN FIZIKAL ..... 77**
**7.1: Perimeter Keselamatan Fizikal ..... 77**
**7.2: Kemasukan Fizikal ..... 78**
7.2.1: Kawalan Masuk Fizikal ..... 78
7.2.2: Keselamatan Persekitaran ..... 79
7.2.3: Kawalan Kawasan Penghantaran Barangan dan *Loading Area* ..... 79
**7.3: Keselamatan Pejabat, Bilik, Dan Kemudahan ..... 79**
**7.4: Pemantauan Keselamatan Fizikal ..... 79**
**7.5: Perlindungan Fizikal Dan Ancaman Persekitaran ..... 80**
**7.6: Bekerja Di Kawasan Yang Selamat ..... 81**
7.6.1: Kawasan Larangan ..... 81
**7.7: Dasar Meja Kosong Dan Skrin Kosong ..... 82**
**7.8: Lokasi Dan Perlindungan Peralatan ..... 83**
**7.9: Keselamatan Aset di Luar Premis ..... 86**
**7.10: Media Storan ..... 87**
**7.11: Utiliti Sokongan ..... 88**
**7.12: Keselamatan Kabel ..... 89**
**7.13: Penyelenggaraan Perkakasan ..... 89**
**7.14: Pelupusan Selamat Atau Penggunaan Semula Peralatan ..... 90**

**BIDANG 8 – KAWALAN TEKNOLOGI ..... 93**

**8.1: Peranti Akhir Pengguna ..... 93**
**8.2: Hak Capaian Istimewa ..... 94**
8.2.1: Pengurusan Hak Capaian Istimewa ..... 94
**8.3: Sekatan Capaian Maklumat ..... 94**
**8.4: Capaian Kepada Kod Sumber ..... 95**
8.4.1: Pembangunan Aplikasi Secara *Outsource* ..... 96
**8.5: Pengesahan Keselamatan Lepas rehat (*Secure Authentication*) ..... 96**
**8.6: Pengurusan Kapasiti ..... 97**
**8.7: Perlindungan Terhadap Perisian *Malware* ..... 98**
**8.8: Pengurusan Kelemahan Teknikal ..... 99**
**8.9: Pengurusan Konfigurasi ..... 100**
**8.10: Pemadaman Maklumat ..... 101**
**8.11: Penyamaran Data ..... 103**
**8.12: Pencegahan Kebocoran Data ..... 104**
**8.13: Sandaran Maklumat ..... 104**
**8.14: Kemudahan Pemprosesan Maklumat Yang Bertindih ..... 105**
**8.15: Log ..... 106**
**8.16: Aktiviti Pemantauan ..... 107**
**8.17: Penyegerakkan Jam ..... 108**
**8.18: Keistimewaan Penggunaan Program Utiliti ..... 108**
**8.19: Pemasangan Perisian Pada Sistem Operasi ..... 108**
**8.20: Kawalan Keselamatan Rangkaian ..... 111**
8.20.1: Kawalan Infrastruktur Rangkaian ..... 111
**8.21: Keselamatan Perkhidmatan Rangkaian ..... 112**
**8.22: Pengasingan Rangkaian ..... 112**
**8.23: Tapisan Laman Web ..... 113**
**8.24: Penggunaan Kriptografi ..... 113**
8.24.1: Enkripsi ..... 113
8.24.2: Tandatangan Digital ..... 113
**8.25: Kitaran Hidup Pembangunan Yang Selamat ..... 114**
**8.26: Keperluan Keselamatan Aplikasi ..... 114**
**8.27: Prinsip Senibina Sistem dan Kejuruteraan Yang Selamat ..... 115**
**8.28: Pengekodan Selamat ..... 116**
**8.29: Ujian Keselamatan Dalam Pembangunan Dan Penerimaan ..... 119**
**8.30: Pembangunan Sumber Luar ..... 120**
**8.31: Pengasingan Persekitaran Pembangunan, Pengujian Dan Pengeluaran ..... 122**
**8.32: Pengurusan Perubahan ..... 123**
8.32.1: Kawalan Perubahan Perkakasan ICT ..... 123

8.32.2: Kawalan Perubahan Sistem ICT ..... 124
**8.33: Maklumat Ujian..... 125**
**8.34: Perlindungan Sistem Maklumat Semasa Pengujian Audit..... 126**
**LAMPIRAN 1..... 129**
**LAMPIRAN 2..... 130**
**BORANG C: BORANG PERMOHONAN/ PERUBAHAN SISTEM/ OPERASI ICT ..... 131**
**BORANG J: PENAMATAN AKAUN APLIKASI DAN PEMULANGAN PERALATAN ICT..... 132**
**GLOSARI ..... 133**

## PENGENALAN

Dokumen Polisi Keselamatan Siber (PKS) ini menggariskan peraturan-peraturan yang perlu dipatuhi oleh pengurusan dan kakitangan yang berkaitan dengan penggunaan dan pengurusan ICT untuk kegunaan di jabatan/ agensi Kerajaan Negeri Melaka. Walau bagaimanapun, jabatan/ agensi boleh menggunapakai Polisi Keselamatan Siber masing-masing mengikut kesesuaian.

## OBJEKTIF

Polisi Keselamatan Siber Negeri Melaka diwujudkan untuk mencapai tahap keselamatan ICT yang menyeluruh bagi memastikan kesinambungan serta perkongsian maklumat dalam semua urusan di pejabat dengan melindungi kepentingan pejabat dan meminimumkan insiden keselamatan ICT serta kesannya seperti berikut:

a. Menerangkan kepada semua pengguna merangkumi warga jabatan/ agensi, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan/ agensi mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber.

b. Memastikan keselamatan penyampaian perkhidmatan jabatan/ agensi di tahap tertinggi sekali gus meningkatkan tahap keyakinan pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;

c. Memastikan kelancaran operasi dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;

d. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

e. Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

**PERNYATAAN DASAR**

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

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

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

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

a) Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
b) Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;
c) Tidak Boleh Disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
d) Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya; dan
e) Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

**SKOP**

Polisi ini meliputi semua sumber atau aset ICT jabatan/ agensi yang terdiri daripada perkakasan, perisian, aplikasi, data, maklumat dan modal insan.

## PRINSIP-PRINSIP POLISI KESELAMATAN SIBER NEGERI MELAKA

Polisi Keselamatan Siber Negeri Melaka diwujudkan mengikut prinsip-prinsip di bawah:

### 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 akses di bawah prinsip ini adalah berasaskan kepada klasifikasi maklumat dan tapisan keselamatan pengguna.

### b. Hak Akses Minimum

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

### c. Kebertanggungjawaban / Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mempunyai keupayaan untuk mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan kata laluan;

v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.

**d. Pengauditan Keselamatan**

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 (*server*), peralatan keselamatan dan rangkaian serta sistem aplikasi hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau jejak audit. Rekod audit hendaklah dilindungi dan tersedia untuk penilaian atau tindakan serta merta. Kebolehan dalam mengakses jejak audit bagi setiap aset ICT, hanyalah terhad dan terbatas kepada Pentadbir Sistem sahaja.

**e. Pemulihan**

Pemulihan sistem/ aset ICT amat diperlukan bagi memastikan ketersediaan (*availability*) dan kebolehcapaian (*accessability*). Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan melalui pendekatan.

**f. Pematuhan**

Pematuhan kepada Polisi Keselamatan Siber Negeri Melaka boleh dicapai melalui tindakan berikut:

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

ii. Merumuskan pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenal pasti;

iii. Melaksanakan program pemantauan keselamatan secara berterusan untuk memastikan standard, prosedur dan garis panduan keselamatan dipatuhi; dan

iv. Menguatkuasakan amalan melaporkan sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan dan pengukuhan.

**PENILAIAN RISIKO KESELAMATAN ICT**

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

Penilaian risiko keselamatan ICT hendaklah dilaksanakan secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT dilaksanakan ke atas aset ICT termasuklah di premis yang menempatkan sumber-sumber teknologi maklumat seperti pusat data, pusat pemulihan bencana, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

Jabatan/ Agensi bertanggungjawab untuk melaksanakan dan menguruskan risiko keselamatan ICT ini adalah selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

Tindakan yang sewajarnya perlu dikenalpasti bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

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

| PERKARA | PERANAN |
|---|---|
| **BIDANG 5: KAWALAN ORGANISASI** | |
| **5.1: Polisi Keselamatan Maklumat** | |
| **Tujuan:**<br>Menerangkan hala tuju, sokongan pengurusan dan peraturan-peraturan terhadap keselamatan maklumat bagi melindungi maklumat dan aset ICT selaras dengan keperluan fungsi-fungsi utama Jabatan/ agensi dan perundangan yang berkaitan. | |
| **5.1.1: Objektif Dasar** | |
| Dasar-dasar yang meliputi perkara-perkara berikut telah ditentukan bagi memenuhi objektif Polisi Keselamatan Siber Negeri Melaka:<br>a) Pembangunan dan Penyelenggaraan Polisi Keselamatan Siber<br>b) Organisasi Keselamatan<br>c) Pengurusan Aset<br>d) Keselamatan Sumber Manusia<br>e) Keselamatan Fizikal Dan Persekitaran<br>f) Pengurusan Operasi dan Komunikasi<br>g) Kawalan Capaian<br>h) Perolehan, Pembangunan dan Penyelenggaraan Aplikasi<br>i) Pengurusan Pengendalian Insiden Keselamatan<br>j) Pengurusan Kesinambungan Perkhidmatan<br>k) Pematuhan Dasar<br>l) Risikan Ancaman<br>m) Dasar Pencegahan Kebocoran Maklumat. | **Semua** |

| | |
|---|---|
| **5.1.2: Pengesahan Dan Pelaksanaan Dasar** | |
| YB Setiausaha Kerajaan Negeri Melaka bertanggungjawab untuk membuat pengesahan dan pelaksanaan Polisi Keselamatan Siber dibantu oleh Jawatankuasa Pemandu ICT (JPICT) Negeri Melaka yang terdiri daripada Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO) dan semua Ketua Jabatan/ Agensi Negeri Melaka. | **SUK/ Pegawai yang diturunkan kuasa** |
| **5.1.3: Penyebaran Dan Perakuan Dasar** | |
| Dasar ini disebarkan kepada semua pengguna Jabatan/ Agensi (termasuk kakitangan, pembekal, pakar runding dan lain-lain) menggunakan platform yang boleh dicapai oleh pihak berkaitan seperti Portal Rasmi Kerajaan Negeri Melaka, e-mel, serahan hardcopy atau lain-lain medium komunikasi dan penerimaan akuan Aku Janji pematuhan dasar. | **CDO** |
| **5.1.4: Penyelenggaraan Dasar** | |
| Dasar ini akan disemak dan dipinda dari semasa ke semasa selaras dengan kemajuan teknologi dan perubahan pada prosedur, perundangan dan perkembangan sosial.<br>Prosedur berhubung penyelenggaraan Polisi Keselamatan Siber Kerajaan Negeri Melaka adalah:<br>a) Mengenal pasti dan menentukan perubahan yang diperlukan;<br>b) Mengemukakan cadangan pindaan untuk mendapatkan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT) Negeri Melaka;<br>c) Memaklumkan perubahan yang telah dipersetujui oleh Mesyuarat Jawatankuasa Pemandu ICT (JPICT) Negeri Melaka kepada semua pengguna; | **ICTSO** |

| | |
|---|---|
| d) Dasar ini hendaklah dikaji atau dikemaskini sekurang-kurangnya dua tahun sekali atau mengikut keperluan dan perubahan ketara bagi memastikan dokumen sentiasa relevan dan berkesan. | |
| **5.1.5: Pengecualian Dasar** | |
| Polisi Keselamatan Siber Kerajaan Negeri Melaka terpakai kepada semua pengguna ICT Jabatan/ agensi dan tiada pengecualian diberikan. | **Semua** |
| **5.2: Tanggungjawab Dan Peranan Dalam Keselamatan Maklumat** | |
| **Tujuan:**<br>Menjelaskan peranan dan tanggungjawab setiap individu yang terlibat secara lebih jelas dan teratur bagi memastikan pencapaian objektif Polisi Keselamatan Siber. | |
| **5.2.1: Setiausaha Kerajaan Negeri (SUK)** | |
| **Peranan** :<br>a) Memperakukan / meluluskan dokumen Polisi Keselamatan Siber Negeri Melaka;<br>b) Memantau tahap pematuhan keselamatan ICT;<br>c) Memperakukan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam Jabatan/ agensi yang mematuhi keperluan Polisi Keselamatan Siber Negeri Melaka;<br>d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT;<br>e) Memastikan Polisi Keselamatan Siber Negeri Melaka selaras dengan dasar-dasar ICT kerajaan semasa;<br>f) Menerima laporan dan membincangkan hal-hal keselamatan Siber semasa;<br>g) Membincangkan tindakan yang melibatkan pelanggaran Polisi Keselamatan Siber Negeri Melaka; dan | **SUK** |

| | |
|---|---|
| h) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden. | |
| **5.2.2: Ketua Pegawai Digital (CDO)** | |
| Peranan dan tanggungjawab Ketua Pegawai Digital (CDO) di semua Jabatan dan Agensi Kerajaan Negeri adalah seperti berikut: Peranan dan tanggungjawab CDO adalah seperti berikut:-<br>a) Membantu Setiausaha Kerajaan Negeri dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;<br>b) Menentukan keperluan keselamatan ICT;<br>c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan maklumat; dan<br>d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT. | **CDO** |
| **5.2.3: Pegawai Keselamatan ICT (ICTSO)** | |
| Peranan dan tanggungjawab ICTSO di semua Jabatan/ agensi Negeri yang dilantik adalah seperti berikut:<br>a) Membantu mengurus program-program keselamatan ICT;<br>b) Menguatkuasakan pelaksanaan Polisi Keselamatan Siber;<br>c) Memberi penerangan dan pendedahan berkenaan Polisi Keselamatan Siber kepada semua pengguna;<br>d) Menjalankan pengurusan risiko dan Keselamatan ICT;<br>e) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan Jabatan/ Agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya;<br>f) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti *virus* dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; | **ICTSO** |

| | |
|---|---|
| g) Menentukan tahap keutamaan insiden, melaporkan insiden keselamatan ICT kepada Pasukan CSIRT Negeri dan memaklumkan kepada CDO serta mengambil langkah pemulihan awal;<br>h) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;<br>i) Membantu menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT;<br>j) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan;<br>k) Memastikan pematuhan Polisi Keselamatan Siber Negeri Melaka oleh pihak luaran seperti perunding, kontraktor dan pembekal yang mencapai dan menggunakan aset ICT untuk tujuan penyelenggaraan, pemasangan, naik taraf dan sebagainya; dan<br>l) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan maklumat. | |
| **5.2.4: Jawatankuasa Pemandu ICT (JPICT) Negeri Melaka** | |
| Jawatankuasa Pemandu ICT (JPICT) bertanggungjawab dalam keselamatan ICT. Keanggotaan adalah seperti berikut:-:<br>Pengerusi : Setiausaha Kerajaan Negeri (SUK)<br>Urusetia : BTMK<br>Ahli : Ketua Jabatan/ Agensi Kerajaan Negeri Melaka | **Ahli JPICT** |

| | |
|---|---|
| **Peranan** :<br>a) Menentukan arah tuju keselamatan Polisi Keselamatan Siber;<br>b) Menilai, melulus dan menguatkuasakan Polisi Keselamatan Siber;<br>c) Memastikan pengauditan sistem ICT dilaksanakan;<br>d) Meneliti dan meluluskan program dan aktiviti berkaitan keselamatan Siber ;<br>e) Memantau ancaman-ancaman utama keselamatan Siber ;<br>f) Melaporkan insiden keselamatan Siber yang telah berlaku dan tindakan yang telah diambil kepada pihak pengurusan; dan<br>g) Menyelenggara Dokumen Polisi Keselamatan Siber Negeri Melaka. | |
| **5.2.5: Cyber Security Incident Response Team (CSIRT)** | |
| **CSIRT Negeri**<br>Keahlian jawatankuasa CSIRT negeri adalah seperti berikut<br>• Timbalan Setiausaha Kerajaan (Pembangunan) -Pengerusi (CDO)<br>• Ketua ICT Negeri<br>• Ketua Penolong Pengarah (KPP) (ICTSO)<br>• Wakil Bahagian Komunikasi Korporat, JKMM<br>• Wakil Unit Dewan & MMKN, JKMM<br>• Wakil Bahagian Khidmat Pengurusan, JKMM<br>• Wakil Majlis Sukan Negeri, JKMM<br>• Wakil Tabung Pendidikan Amanah Negeri Melaka, JKMM<br>• Wakil Pejabat Penasihat Undang-Undang Negeri<br>• Wakil Pejabat Kewangan & Perbendaharaan Negeri<br>• Wakil Pejabat Pembangunan Persekutuan Negeri<br>• Wakil Jabatan Mufti Negeri Melaka<br>• Wakil Mahkamah Syariah Melaka | **CSIRT Negeri** |

| | |
|---|---|
| • Wakil Pejabat Pengarah Tanah dan Galian Negeri Melaka<br>• Wakil Jabatan Kerja Raya Melaka<br>• Wakil Pejabat Daerah dan Tanah Melaka Tengah<br>• Wakil Pejabat Daerah dan Tanah Alor Gajah<br>• Wakil Pejabat Daerah dan Tanah Jasin<br>• Wakil Pertanian Negeri Melaka<br>• Wakil Jabatan Agama Islam Melaka<br>• Wakil Kebajikan Masyarakat<br>• Wakil Jabatan Perkhidmatan Veterinar<br>• Wakil Perancang Bandar dan Deşa Negeri Melaka<br>• Wakil Majlis Bandaraya Melaka Bersejarah<br>• Wakil Majlis Perbandaran Alor Gajah<br>• Wakil Majlis Perbandaran Jasin<br>• Wakil Majlis Perbandaran Hang Tuah Jaya<br>• Wakil Lembaga Perumahan Melaka<br>• Wakil Perbadanan Melaka (MCORP)<br>• Wakil Yayasan Melaka<br>• Wakil Perbadanan Muzium Melaka<br>• Wakil Perbadanan Perpustakaan Awam Melaka<br>• Wakil Perbadanan Bioteknologi Melaka<br>• Wakil Majlis Agama Islam Melaka<br><br>Peranan dan Tanggungjawab CSIRT Negeri adalah seperti berikut:<br>a) Memantau, mengesan insiden, menerima dan mengesahkan aduan insiden keselamatan siber, seterusnya mengenal pasti jenis insiden serta menilai impak insiden keselamatan siber;<br>b) Merekod dan menjalankan siasatan awal terhadap insiden yang diterima;<br>c) Melaksanakan pengurusan dan pengendalian insiden keselamatan siber serta mengambil tindakan awal pemulihan;<br>d) Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan serta pengukuhan keselamatan siber supaya insiden baharu dapat dielakkan; | |

| | |
|---|---|
| e) Menasihat agensi di bawah seliaannya mengambil tindakan pemulihan dan pengukuhan;<br>f) Menyebarkan makluman/amaran berkaitan insiden kepada agensi lain di bawah seliaannya; dan<br>g) Memastikan fail log disimpan sekurang-kurangnya enam bulan di tempat yang selamat.<br><br>**<u>CSIRT Agensi</u>**<br><br>Keahlian Jawatankuasa CSIRT Agensi ditentukan oleh Agensi masing-masing berpandukan kepada Pekeliling Am Bil. 4 Tahun 2022 dan pekeliling-pekeliling yang berkaitan. | |
| **5.2.6: Pengguna** | |
| Peranan dan tanggungjawab pengguna adalah:-<br>a) Membaca, memahami, menandatangani dan mematuhi Polisi Keselamatan Siber Negeri Melaka;<br>b) Mengetahui dan memahami implikasi keselamatan maklumat, kesan dari tindakannya dan penglibatan dalam memenuhi keperluan sistem pengurusan keselamatan maklumat;<br>c) Melaksanakan prinsip-prinsip Polisi Keselamatan Siber dan menjaga kerahsiaan maklumat Jabatan/ Agensi; dan<br>d) Melaksanakan langkah-langkah perlindungan seperti berikut :-<br>i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;<br>ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;<br>iii. Menentukan maklumat sedia untuk digunakan;<br>iv. Menjaga kerahsiaan kata laluan;<br>v. Mematuhi prosedur, langkah dan garis panduan keselamatan yang ditetapkan; | **Semua** |

| | |
|---|---|
| vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;<br>vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum; dan<br>viii. Melaporkan sebarang aktiviti yang mengancam keselamatan maklumat kepada ICTSO dengan segera.;<br>ix. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat;<br>x. Menghadiri dan melibatkan diri di dalam program/aktiviti kesedaran mengenai keselamatan maklumat; dan<br>xi. Menandatangani Borang Akuan Pematuhan Polisi Keselamatan Siber Negeri Melaka dan Sistem Pengurusan Keselamatan Maklumat (ISMS) sebagaimana **LAMPIRAN 2**. | |
| **5.2.7: Juru Audit Dalaman** | |
| Juru Audit Dalaman bertanggungjawab mengaudit sistem dan proses pengurusan keselamatan ICT di seluruh Jabatan/ Agensi dan mencadangkan langkah-langkah pembetulan. | **Juru Audit Dalaman** |
| **5.2.8: Pihak Ketiga** | |
| Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (pembekal, pakar runding dan lain-lain) bagi memastikan penggunaan maklumat dan kemudahan proses maklumat termasuk yang berikut:-:<br>a) Membaca, memahami dan mematuhi Polisi Keselamatan Siber Negeri Melaka;<br>b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; | **Pihak Ketiga** |

| | |
|---|---|
| c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga;<br>d) Memastikan akses kepada aset ICT Jabatan/ Agensi perlu berlandaskan kepada perjanjian kontrak;<br>e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai.<br>i. *Perakuan Akta Rahsia Rasmi 1972;* dan<br>ii. Hak Harta Intelek.<br>f) Pihak ketiga perlu mematuhi Polisi Keselamatan Jabatan/ Agensi serta menandatangani *Non-Disclosure Agreement (NDA)*;<br>g) Menandatangani Borang Akuan Pematuhan Polisi Keselamatan Siber Negeri Melaka dan Sistem Pengurusan Keselamatan Maklumat (ISMS) sebagaimana **LAMPIRAN 2**; dan<br>h) Langkah-langkah harus diambil bagi memastikan segala peraturan atau dasar yang dipatuhi oleh pihak ketiga juga diambil kira bagi seluruh "*supply chain*" (contohnya, sub-kontraktor). | |
| **5.3: Pengasingan Tugas** | |
| **Objektif:**<br>Menerangkan tugas dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur bagi mengurangkan risiko penipuan, kesilapan serta pemintasan (*bypassing*) kawalan keselamatan maklumat. | |
| **5.3.1: Pentadbir Sistem Aplikasi** | |
| Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut:-: | **Pentadbir Sistem Aplikasi** |

| | |
|---|---|
| a) Pengurusan Akses – Mengawal dan menetapkan tahap capaian pengguna bagi memastikan hanya individu yang diberi kebenaran boleh mengakses sistem;<br>b) Pemantauan& Pengesanan Ancaman – Memantau aktiviti sistem secara berkala serta mengenal pasti dan bertindak terhadap sebarang ancaman keselamatan;<br>c) Penyulitan& Perlindungan Data – Melaksanakan mekanisme penyulitan bagi melindungi data sensitif daripada akses tanpa kebenaran;<br>d) Pengurusan Kemas Kini& Tampalan Keselamatan – Memastikan sistem sentiasa dikemas kini dengan tampalan keselamatan terkini bagi mengelakkan eksploitasi kelemahan;<br>e) Pengurusan Insiden Keselamatan – Menyediakan pelan tindak balas terhadap insiden keselamatan serta memastikan pemulihan segera sekiranya berlaku pelanggaran keselamatan; dan<br>f) Penyelenggaraan Rekod Audit (*audit trail*) – Menyimpan dan menganalisis rekod audit (mengikut keperluan) bagi memastikan ketelusan serta mengesan sebarang aktiviti mencurigakan. | |
| **5.3.2: Pentadbir Rangkaian** | |
| Pentadbir Rangkaian adalah bertanggungjawab melaksanakan perkara-perkara berikut :<br>a. Memastikan rangkaian Melaka*Net, rangkaian setempat (LAN), rangkaian luas (WAN) dan rangkaian lain yang menyokong operasi Pentadbiran Kerajaan Negeri Melaka beroperasi sepanjang masa;<br>b. Merancang dan melaksanakan peningkatan infrastruktur, keselamatan dan prestasi rangkaian sedia ada; | **Pentadbir Rangkaian** |

| | |
|---|---|
| c. Memantau prestasi rangkaian dan memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan baik;<br>d. Mengesan dan mengambil tindakan pembaikan segera ke atas sebarang kerosakan peralatan rangkaian;<br>e. Memantau penggunaan rangkaian dan melaporkan kepada CSIRT Negeri Melaka sekiranya berlaku penyalahgunaan sumber rangkaian;<br>f. Mewartakan polisi dan garis panduan penggunaan rangkaian komputer kepada semua pengguna rangkaian;<br>g. Memastikan laluan trafik rangkaian komputer keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan luar ke dalam rangkaian Pejabat Pentadbiran Kerajaan Negeri Melaka secara tidak sah; dan<br>h. Menyiasat dan menyelesaikan masalah rangkaian serta memberikan sokongan teknikal kepada pengguna untuk menyelesaikan masalah yang berkaitan dengan rangkaian. | |
| **5.3.3: Pentadbir Laman Web** | |
| Pentadbir Laman Web bertanggungjawab melaksanakan perkara-perkara berikut:<br>a) Pengurusan Kandungan – Memastikan maklumat yang dipaparkan sentiasa terkini, tepat, dan relevan dengan keperluan pengguna. Hanya kandungan yang telah disemak dan disahkan sahaja yang akan dimuat naik;<br>b) Pematuhan Dasar dan Garis Panduan – Memastikan laman web mematuhi dasar kerajaan dan garis panduan rasmi berkaitan pengurusan laman web sektor awam serta memenuhi kriteria penilaian yang ditetapkan dalam Sistem Pemantauan Laman Web dan Servis Kerajaan (SPLASK); | **Pentadbir Laman Web** |

| | |
|---|---|
| c) Keselamatan Portal – Melaksanakan langkah-langkah keselamatan seperti kawalan akses, penyulitan data, dan pemantauan ancaman siber bagi melindungi maklumat pengguna;<br>d) Penyelenggaraan Teknikal – Memastikan laman web berfungsi dengan baik, termasuk kemas kini perisian, pembaikan pepijat, dan peningkatan prestasi;<br>e) Pemantauan& Penilaian – Melakukan audit berkala terhadap prestasi laman web, termasuk analisis trafik dan kepuasan pengguna; dan<br>f) Pengurusan Krisis& Pemulihan – Menyediakan dokumentasi tentang konfigurasi laman web, perubahan yang dilakukan, masalah dan penyelesaiannya, serta pelan pemulihan bencana. | |
| **5.3.4: Pentadbir E-mel** | |
| Pentadbir E-mel memainkan peranan penting dalam memastikan kelancaran, keselamatan, dan kecekapan sistem komunikasi e-mel organisasi. Skop tanggungjawab merangkumi:<br>a) Pengurusan Akaun Pengguna: Mengurus penciptaan, penyelenggaraan dan penamatan akaun e-mel, serta menetapkan kebenaran akses mengikut peranan pengguna. Pentadbir e-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib;<br>b) Konfigurasi dan Pemantauan Sistem: Melaksanakan pemasangan, konfigurasi, penyelenggaraan serta pemantauan berterusan terhadap prestasi pelayan dan aplikasi e-mel;<br>c) Memastikan kemudahan membuat capaian e-mel melalui pelbagai media seperti telefon mudah alih disediakan kepada pengguna e-mel; | **Pentadbir E-mel** |

| | |
|---|---|
| d) Keselamatan Sistem: Melaksanakan mekanisme keselamatan seperti pengesahan dua faktor (sekiranya ada), enkripsi, kawalan akses, serta pengesanan dan pencegahan ancaman seperti spam dan phishing;<br>e) Pengurusan Antaramuka Pengguna: Menyesuaikan paparan, susun atur dan fungsi antara muka pengguna bagi memastikan pengalaman penggunaan yang efisien dan mesra pengguna;<br>f) Penyelenggaraan Kandungan Komunikasi: Mengurus kandungan komunikasi rasmi seperti pengumuman dalaman, notifikasi dan siaran organisasi melalui sistem e-mel;<br>g) Pematuhan dan Pemantauan Keselamatan: Memastikan sistem e-mel mematuhi dasar keselamatan ICT dan garis panduan berkaitan, serta melaporkan sebarang insiden keselamatan;<br>h) Integrasi Aplikasi: Menyokong integrasi sistem e-mel dengan aplikasi lain seperti kalendar, kolaborasi, sistem notifikasi dan pangkalan data pengguna;<br>i) Sokongan Teknikal: Memberi khidmat sokongan dan latihan kepada pengguna dalam menyelesaikan isu teknikal berkaitan sistem e-mel.<br>j) Kerjasama Pihak Ketiga: Berurusan dengan penyedia perkhidmatan, vendor, dan agensi berkaitan untuk penyelenggaraan, keselamatan dan pematuhan sistem;<br>k) Pengurusan Kumpulan E-mel: Mewujudkan dan menyelenggara kumpulan e-mel berdasarkan keperluan jabatan atau projek untuk memudahkan komunikasi berkumpulan. Mengurus keahlian kumpulan e-mel dengan menambah atau mengeluarkan ahli mengikut perubahan dalam organisasi; dan<br>l) Pengurusan Polisi dan Etika Penggunaan E-mel: Menyediakan polisi penggunaan e-mel rasmi yang jelas, | |

| | |
|---|---|
| termasuk larangan penggunaan untuk tujuan peribadi, dan memastikan semua pengguna mematuhinya. | |
| **5.3.5: Pentadbir Active Directory (AD) / Domain Controller** | |
| Pentadbir Active Directory (AD) atau Domain Controller bertanggungjawab penuh dalam pengurusan, penyelenggaraan dan pemantauan keselamatan sistem direktori bagi memastikan kestabilan, kebolehpercayaan dan kecekapan persekitaran IT organisasi. Skop utama tugas mereka meliputi:<br>a) **Pengurusan Objek Direktori** – Mencipta, mengemaskini dan memadam objek seperti akaun pengguna, kumpulan, komputer dan peranti dalam struktur AD mengikut keperluan operasi;<br>b) **Pengurusan Akses dan Pengguna** – Menyelaras pendaftaran dan penyelenggaraan pengguna serta keahlian kumpulan, termasuk pengurusan hak akses terhadap sumber IT melalui polisi yang ditetapkan;<br>c) **Integrasi Sistem** – Mengurus integrasi AD dengan aplikasi dan perkhidmatan lain untuk memastikan fungsi penyelarasan sistem merentas platform berjalan lancar; dan<br>d) **Sokongan Teknikal** – Menyediakan bantuan teknikal kepada pengguna akhir berkenaan isu capaian dan pentadbiran dalam sistem AD.<br><br>Pentadbir AD memainkan peranan penting dalam memastikan struktur direktori organisasi sentiasa berada dalam keadaan optimum dan selamat. | **Pentadbir Active Directory (AD) / Domain Controller** |

| 5.3.6: Pentadbir Pangkalan Data | |
|---|---|
| Berikut adalah tiga (3) peranan utama Pentadbir Pangkalan Data (DBA) mengikut pembahagian:<br><br>a) Pasukan Pusat Data (Infra DBA):<br><br>i. Penyelenggaraan dan Pemantauan Sistem DBMS:<br>• Memastikan pangkalan data sentiasa tersedia, stabil dan berprestasi tinggi.<br>• Mengurus ruang storan, tampungan beban, dan penalaan prestasi (*performance tuning*).<br><br>ii. Keselamatan dan *backup* Pangkalan Data:<br>• Melaksanakan *backup* harian/berkala serta ujian pemulihan data (*restore testing*).<br>• Mengurus kawalan akses keseluruhan kepada pangkalan data mengikut tahap sensitiviti.<br>iii. Naik Taraf dan Tampalan Keselamatan (*Patching*):<br>• Melaksanakan *upgrade* DBMS dan patch keselamatan mengikut garis panduan *vendor* dan dasar keselamatan organisasi.<br>b) Pasukan Aplikasi (Apps DBA):<br>i. Reka Bentuk dan Struktur Data:<br>• Menyusun struktur jadual, indeks, prosedur tersimpan (*stored procedure*) dan hubungan relasi mengikut keperluan aplikasi.<br>ii. Pengurusan Prestasi Aplikasi Berasaskan Data:<br>• Menyemak dan mengoptimumkan SQL query yang digunakan oleh aplikasi.<br>• Bekerjasama dengan pasukan infra untuk menangani masalah *bottleneck* aplikasi.<br>iii. Ujian dan Sokongan Naik Taraf Aplikasi:<br>• Menguji fungsi aplikasi selepas perubahan pada skema atau versi DBMS. | **Pentadbir Pangkalan Data** |

| | |
|---|---|
| • Memberi sokongan teknikal semasa deployment atau migrasi aplikasi.<br>Peranan ini saling berkait dan memerlukan kerjasama antara pasukan pusat data dan aplikasi untuk memastikan keseluruhan sistem berfungsi lancar. | |
| **5.3.7: Pentadbir *Backup* Data** | |
| Pentadbir *Backup* Data bertanggungjawab untuk merancang, mengkonfigurasi, mengurus, dan memantau operasi serta pemulihan data dalam sistem *backup* organisasi. Berikut adalah beberapa aspek utama dari skop kerja mereka:<br>a) Merancang Sistem *backup*: Menganalisis keperluan penyimpanan dan keperluan pemulihan data organisasi untuk merancang sistem *backup* yang sesuai, termasuk pemilihan teknologi, peranti, dan perisian yang sesuai;<br>b) Pemasangan dan Konfigurasi: Memasang, mengkonfigurasi, dan menguruskan perisian dan peranti *backup*, termasuk pelayan *backup*, storan jaringan (NAS), penyimpanan teras, dan peranti penyimpanan lainnya;<br>c) Penjadualan Backup: Menjadualkan operasi *backup* secara berkala untuk memastikan data organisasi disalin dengan teratur dan dikekalkan dalam keadaan yang konsisten;<br>d) Pemantauan Operasi *Backup*: Memantau operasi *backup* secara berkala untuk memastikan bahawa proses berjalan seperti yang dijangka, serta mengenal pasti dan menyelesaikan masalah yang timbul dengan segera.<br>e) Pengurusan Kapasiti: Mengurus kapasiti penyimpanan Backup dan merancang strategi retensi data untuk memastikan penyimpanan yang efisien dan pemulihan data yang sesuai dengan peraturan dan keperluan organisasi;<br>f) Pemulihan Data: Menyelenggarakan ujian pemulihan dan menjalankan operasi pemulihan data apabila diperlukan, | **Pentadbir *Backup* Data** |

| | |
|---|---|
| termasuk pemulihan sebahagian atau sepenuhnya data dari salinan *backup*; dan<br>g) Keselamatan Data: Memastikan keselamatan data dalam salinan *backup* dengan melaksanakan kawalan akses, enkripsi data, dan langkah-langkah keselamatan lainnya untuk melindungi daripada kehilangan atau akses tidak dibenarkan. | |
| **5.3.8: Pegawai Aset ICT Dan Pentadbir Teknikal** | |
| Peranan dan tanggungjawab pegawai aset ICT dan Pentadbir Teknikal adalah seperti berikut:<br>a) Pemantuan aset ICT: Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, tablet, pencetak, pengimbas dan sebagainya berada dalam keadaan yang baik;<br>b) Memastikan aset ICT milik Kerajaan Negeri Melaka dilabelkan dan direkod;<br>c) Pemeriksaan dan Penyelenggaraan: Memastikan aset milik Kerajaan Negeri Melaka dibuat pemeriksaan berkala secara tahunan dan diselenggara sebaiknya agar dapat meningkatkan jangka hayat aset ICT tersebut;<br>d) Penyimpanan Aset ICT: Memastikan aset ICT untuk kegunaan pinjaman dan simpanan sebelum agihan diletakkan di dalam bilik stor yang mempunyai kawalan keselamatan yang terjamin;<br>e) Ketersediaan Stok Alat Ganti : Memastikan stok alat ganti aset ICT sentiasa mencukupi dan disimpan di tempat yang selamat dan terkawal; dan<br>f) Pelupusan Aset ICT: Memastikan aset ICT yang ingin dilupuskan dilaksanakan mengikut garis panduan kawalan keselamatan bagi pelupusan data digital. | **Pegawai Aset ICT dan Pentadbir Teknikal** |

| | |
|---|---|
| Peranan dan tanggungjawab Pentadbir Teknikal adalah seperti berikut:<br>a) Penyediaan Sokongan Teknikal: Menyediakan khidmat sokongan teknikal ICT;<br>b) Perolehan Aset ICT: Merancang dan melaksanakan perolehan aset dan alat ganti ICT;<br>c) Pengurusan Aset ICT: Mengurus penerimaan, pendaftaran, agihan, penempatan dan pelupusan aset ICT;<br>d) Penyelenggaraan Berkala: Memastikan semua aset ICT diselenggara secara berkala dengan baik;<br>e) Pemasangan Perisian Keselamatan: Memastikan perisian antivirus dipasang pada aset ICT; dan<br>f) Pengurusan Meja Bantuan Teknikal: Mengurus Meja Bantuan ICT Kerajaan Negeri Melaka melalui Sistem Intranet Melaka*Net Sistem Intranet Negeri Melaka– Modul Aduan Kerosakan Peralatan ICT atau sistem sistem yang setara. | |
| **5.3.9: Pentadbir Pusat Data** | |
| Peranan Pentadbir Pusat Data adalah seperti berikut;<br>a) Memastikan persekitaran fizikal dan keselamatan pusat data dan Pusat Pemulihan bencana berada dalam keadaan baik dan selamat;<br>b) Memastikan operasi Pusat Data dan DRC berada dalam keadaan baik 24 x 7;<br>c) Memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data dan Pusat Pemulihan bencana;<br>d) Memantau aset ICT sokongan dan fasiliti sokongan (*precision aircond*, alat pencegah kebakaran, *alarm*, bekalan elektrik) di Pusat Data dan DRC bagi memastikan beroperasi lancar 24 x 7; | **Pentadbir Pusat Data** |

| | |
|---|---|
| e) Menjadualkan dan melaksanakan proses *backup* dan *restoration* ke atas pangkalan data dan sistem secara berkala;<br>f) Menyediakan perancangan Pelan Pemulihan Bencana;<br>g) Memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa;<br>h) Melaporkan sebarang insiden pelanggaran dasar keselamatan pusat data kepada ICTSO;<br>i) Menguruskan permohonan baru dan pengemaskinian *server* atau *virtual machine* bagi sistem aplikasi baru di Pusat Data dan DRC; dan<br>j) Menguruskan khidmat sokongan operasi *server* dari segi penerimaan, penyediaan, penyelenggaraan, waranti, pengeluaran dan pelupusan. | |
| **5.4: Tanggungjawab Pengurusan** | |
| **Objektif:**<br>Untuk memastikan pengurusan memahami peranan mereka dalam keselamatan maklumat dan melaksanakan tindakan yang bertujuan untuk memastikan semua kakitangan menyedari dan memenuhi tanggungjawab keselamatan maklumat mereka. | |
| **5.4.1: Pengurusan Tertinggi** | |
| Peranan dan tanggungjawab pengurusan tertinggi adalah bagi memastikan perkara-perkara berikut:-:<br>a) Semua pengguna memahami Polisi Keselamatan Siber Negeri Melaka yang telah ditetapkan;<br>b) Semua pengguna mematuhi Polisi Keselamatan Siber Negeri Melaka;<br>c) Perlindungan keselamatan adalah mencukupi dari setiap aspek (sumber kewangan, sumber manusia dan perlindungan keselamatan); dan | **Pengurusan Tertinggi** |

| | |
|---|---|
| d) Program keselamatan maklumat dan penilaian risiko dilaksanakan; | |
| **5.5: Hubungan Dengan Pihak Berkuasa** | |
| **Objektif:**<br>Memastikan komunikasi berkenaan keselamatan maklumat dilaksanakan melalui saluran yang sesuai antara organisasi dan pihak berkuasa, badan perundangan undang-undang dan lain-lain pihak berkuasa yang berkaitan. | |
| Menyediakan Pelan Kesinambungan Perkhidmatan (PKP) bagi memulihkan perkhidmatan supaya Jabatan/ Agensi dapat meneruskan operasi sekiranya berlaku gangguan. PKP hendaklah diurus dan dirangka dengan tepat dengan perbelanjaan yang berpatutan. | **Bahagian Khidmat Pengurusan (BKP)** |
| **5.6: Hubungan Dengan Pihak Berkepentingan** | |
| **Objektif:**<br>Memastikan komunikasi berkaitan dengan kumpulan khusus/ pakar dapat dilaksanakan bagi meningkatkan kemahiran dan pengetahuan berkenaan keselamatan maklumat. | |
| Hubungan dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan seperti Agensi Keselamatan Siber Negara (NACSA), Pejabat Ketua Keselamatan Kerajaan (CGSO), CyberSecurity Malaysia dan lain-lain. | **CDO**<br>**ICTSO**<br>**Pentadbir Sistem Aplikasi** |
| **5.7: Perisikan Ancaman** | |
| **Objektif:**<br>Memastikan kesedaran berkenaan ancaman keselamatan maklumat organisasi dapat dilaksanakan supaya tindakan mitigasi yang bersesuaian dapat diambil. | |

| | |
|---|---|
| Perisikan ancaman adalah tindakan yang diambil untuk mengesan, melindungi, dan mencegah berbagai jenis ancaman keselamatan siber.<br><br>Tindakan yang perlu diambil adalah seperti yang berikut:<br><br>a) Memasang sistem pencegahan pencerobohan (IPS) yang akan mengesan dan mencegah serangan ancaman siber;<br>b) Memasang pendinding api (*Firewall)* bagi mengawal lalu lintas rangkaian berdasarkan peraturan yang ditetapkan;<br>c) Data yang disimpan hendaklah di enkrip;<br>d) Memastikan setiap perisian yang digunakan adalah sah sentiasa dikemaskini;<br>e) Kawalan akses pengguna sistem berdasarkan skop tugas yang telah ditetapkan oleh pemilik sistem;<br>f) Pembahagian rangkaian komputer kepada segmen tertentu bagi mengelak penyebaran kerosakan;<br>g) Menilai dan mengemaskini teknologi peralatan ICT seiring dengan perkembangan semasa; dan<br>h) Perisikan ancaman adalah melibatkan pengumpulan, analisis, dan pelaporan maklumat mengenai ancaman siber. | **Pentadbir Rangkaian** |
| **5.8: Keselamatan Maklumat Di Dalam Pengurusan Projek** | |
| **Objektif:**<br><br>Memastikan risiko keselamatan maklumat telah ditentukan sepanjang projek berlangsung. | |
| Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br><br>a) Elemen keselamatan maklumat perlu diterapkan bagi setiap pengurusan projek; | **Semua** |

| | |
|---|---|
| b) Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek;<br>c) Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan; dan<br>d) Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam Polisi Keselamatan Siber Negeri Melaka. | |
| **5.9: Maklumat Inventori & Aset-aset Lain Yang Berkaitan** | |
| **Objektif:**<br>Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT. | |
| Memastikan semua aset Jabatan/ Agensi Kerajaan Negeri Melaka diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut:<br>a) Mengenal pasti Pegawai Penerima aset setiap unit untuk menguruskan penerimaan aset-aset ICT bagi projek-projek ICT;<br>b) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam Daftar Aset Alih (harta modal, harta modal bernilai rendah dan inventori) & Daftar Aset Tidak Ketara serta sentiasa dikemaskini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa;<br>c) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;<br>d) Pegawai Aset hendaklah mengesahkan penempatan aset ICT; | **Pegawai Penerima Aset, Pegawai Aset ICT** |

| | |
|---|---|
| e) Peraturan bagi pengendalian aset ICT hendaklah dikenalpasti, didokumen dan dilaksanakan;<br>f) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan<br>g) Sebarang perlanggaran peraturan hendaklah dilaporkan kepada Pegawai Aset / ICTSO.<br><br>Aset ICT yang diselenggara adalah hak milik Jabatan/ Agensi. Perkara-perkara yang perlu dipatuhi oleh pemilik aset adalah seperti berikut:<br>a) Memastikan aset ICT di bawah tanggungjawabnya telah dimasukkan dalam senarai aset;<br>b) Memastikan semua aset ICT telah dikelaskan dan dilindungi;<br>c) Mengenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan;<br>d) Memastikan pengendalian aset ICT dilaksanakan dengan baik apabila aset ICT dihapus atau dilupuskan; dan<br>e) Memastikan semua jenis aset ICT dipelihara dengan baik. | **Pegawai Aset ICT dan Semua Pengguna** |
| **5.10: Kebenaran Penggunaan Maklumat Dan Aset Berkaitan** | |
| **Objektif:**<br><br>Memastikan maklumat dan aset lain yang berkaitan dilindungi, digunakan dan dikendalikan dengan sewajarnya. | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:-:<br>a) Aset ICT yang dipinjam oleh pengguna perlulah direkodkan di dalam Sistem Intranet Negeri Melaka*Net – Modul Pinjaman Peralatan ICT atau sistem yang setara (sekiranya ada) dan maklumat pinjaman direkodkan serta dikemas kini; | **Semua** |

| | |
|---|---|
| b) Peminjam aset ICT bertanggungjawab dan memastikan aset yang dipinjam tidak boleh diberi kepada individu atau peminjam lain;<br>c) Pegawai Aset perlu mengenalpasti aset ICT yang dimohon untuk peminjaman dan memastikan aset tersebut berada dalam keadaan baik;<br>d) Pegawai Aset harus bertanggungjawab dan memastikan aset ICT yang dipinjamkan adalah aset yang berdaftar; dan<br>e) Peminjam aset ICT harus mematuhi tatacara pinjaman dan prosedur yang telah ditetapkan oleh Jabatan/ Agensi. | |
| **5.11: Pemulangan Aset** | |
| **Objektif:**<br>Melindungi aset ICT Jabatan/ agensi sebagai sebahagian daripada proses pertukaran unit/ bahagian/jabatan, bersara, penamatan perkhidmatan kakitangan, dan penamatan kontrak atau perjanjian. | |
| Pemulangan bagi peminjaman aset ICT perlulah mematuhi proses-proses yang berikut:<br>a) Peminjam hendaklah memulangkan semula aset ICT sebaik sahaja selesai penggunaan atau tempoh perkhidmatan/ peminjaman telah tamat melalui Sistem Intranet Negeri Melaka*Net – Modul Pinjaman Peralatan ICT atau Sistem Intranet Negeri Melaka*Net – Modul Penamatan Akaun Aplikasi & Pemulangan Peralatan ICT (Borang J) atau mengikut prosedur jabatan/ agensi masing-masing.;<br>b) Pegawai Aset perlu memastikan pemulangan aset yang dipinjam berada dalam keadaan yang baik dan jumlah aksesori yang dibekalkan mencukupi.;<br>c) Pegawai Aset harus merekodkan pemulangan aset di dalam Sistem Intranet Negeri Melaka*Net- Modul Pinjaman Peralatan ICT atau Sistem Intranet Negeri Melaka*Net- Modul Penamatan Akaun Aplikasi & Pemulangan Peralatan | **Semua** |

| | |
|---|---|
| ICT (Borang J) atau mengikut prosedur jabatan/ agensi masing-masing(sekiranya ada) dan dikemaskini oleh kerani bantuan.;<br>d) Jika terdapat kerosakan, peminjam atau Pegawai Aset perlu mengisi borang aduan kerosakan bagi membolehkan proses pembaikan dilakukan.; dan<br>e) Peminjam aset bertanggungjawab sepenuhnya ke atas perkakasan / peralatan / aset ICT dan menggunakan aset ICT tersebut bagi tujuan kerja-kerja rasmi sahaja. | |
| **5.12: Pengelasan Dan Pengendalian Maklumat** | |
| **Objektif:**<br>Memastikan pengenalan dan pemahaman tentang keperluan perlindungan maklumat selaras dengan kepentingannya kepada organisasi. | |
| **5.12.1: Pengelasan Maklumat** | |
| Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian. Maklumat hendaklah dikelaskan dan mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan iaitu :-:<br>a) Rahsia Besar;<br>b) Rahsia;<br>c) Sulit; atau<br>d) Terhad | **Bahagian Teknologi Maklumat dan Komunikasi (BTMK)** |
| **5.12.2: Pengendalian Maklumat** | |
| Langkah-langkah keselamatan perlu diambil kira ketika mengendalikan maklumat seperti mengumpul, menghantar, menyimpan, memproses, menyampai, menukar dan ketika memusnahkan maklumat.<br>Langkah-langkah keselamatan yang perlu diambil adalah:-: | **Semua** |

| | |
|---|---|
| a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;<br>b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;<br>c) Menjaga kerahsiaan kata laluan;<br>d) Nyahaktifkan *"remember me password*";<br>e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;<br>f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;<br>g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum;<br>h) Menentukan maklumat sedia untuk digunakan;<br>i) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan<br>j) Memberi amaran terhadap sebarang ancaman keselamatan ICT seperti serangan *virus*., ransomware, malware, serangan penafian perkhidmatan (DDOS - *Denial of Service*), kecurian data (*identity theft*) dan kejuruteraan sosial (cth *email phishing*). | |
| **5.13: Pelabelan Maklumat** | |
| **Objektif:**<br>Memudahkan komunikasi klasifikasi maklumat dan menyokong automasi maklumat pemprosesan dan pengurusan. | |
| Prosedur Pelabelan maklumat hendaklah dilaksanakan mengikut klasifikasi maklumat yang digunapakai oleh jabatan/ Agensi Negeri. | **Semua** |

| **5.14: Pemindahan Maklumat (*Information Transfer*)** | |
|---|---|
| **Objektif:**<br>Mengekalkan keselamatan maklumat yang dipindahkan di dalam organisasi dan juga pihak ketiga. | |
| **5.14.1: Pemindahan Maklumat** | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br>a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal boleh diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis platform kemudahan komunikasi;<br>b) Terma pemindahan maklumat dan perisian di antara Jabatan/ Agensi dengan pihak luar hendaklah dimasukkan dalam perjanjian;<br>c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari Jabatan/ Agensi; dan<br>d) Melindungi sebaik-baiknya maklumat yang terdapat dalam media. | **Semua** |
| **5.14.2: Penggunaan E-mel** | |
| Penggunaan e-mel dipantau secara berterusan oleh Pentadbir e-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam *Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003* bertajuk *"Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"* dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: | **Semua** |

| | |
|---|---|
| a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh Jabatan/ Agensi sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;<br><br>b) Dalam keadaan yang memudaratkan perkhidmatan Jabatan/ Agensi, penggunaan selain e-mel Jabatan/ Agensi adalah dibenarkan oleh CDO;<br><br>c) Sebarang penghantaran dokumen rasmi hendaklah menggunakan e-mel rasmi Jabatan/ Agensi;<br><br>d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;<br><br>e) Semua e-mel hendaklah melalui proses *scanning* untuk memastikan e-mel yang diterima atau dihantar tidak mempunyai *virus*. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi dua puluh lima megabait (25MB) semasa penghantaran. Kaedah pemampatan (*zip file*) untuk mengurangkan saiz adalah disarankan;<br><br>f) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan serta mengemaskini *mailbox* masing-masing;<br><br>g) Pengguna dinasihatkan tidak membuka e-mel yang mencurigakan;<br><br>h) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;<br><br>i) Maklumat lanjut mengenai keselamatan e-mel bolehlah merujuk kepada *Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003* bertajuk *“Garis Panduan Mengenai* | |

| | |
|---|---|
| *Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan";*<br>j) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;<br>k) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera;<br>l) Menghadkan jenis dan saiz fail lampiran bagi tujuan mengelakkan jangkitan *virus* dan serangan e-mel *bombing*;<br>m) Penggunaan e-mel Jabatan/ Agensi bagi tujuan peribadi adalah tidak dibenarkan;<br>n) Pentadbir e-mel perlu menetapkan had minimum kuota *mailbox*.<br>o) Pembersihan e-mel hendaklah dibuat sekiranya *mailbox* didapati tidak aktif selama tiga (3) bulan atau melebihi kuota dan had masa yang ditetapkan;<br>p) Pengguna adalah dilarang sama sekali menggunakan alamat e-mel rasmi Jabatan/ Agensi bagi pendaftaran dalam mana-mana web/ kumpulan/ forum yang tidak berkaitan dengan urusan kerja rasmi; dan<br>q) Bahagian Sumber Manusia Jabatan/ Agensi perlu memaklumkan sebarang status pengguna (bertukar jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke Jabatan/ Agensi) di bahagian masing-masing bagi tujuan pengemaskinian e-mel yang terlibat.<br>Pelanggaran kepada mana-mana peraturan boleh menyebabkan penggantungan akaun pengguna atau mana-mana tindakan tatatertib yang bersesuaian. | |

| 5.15: Kawalan Capaian | |
|---|---|
| **Objektif:**<br><br>Kawalan capaian bertujuan mengawal capaian pengguna ke atas aset ICT dan melindunginya dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. | |
| **5.15.1: Keperluan Kawalan Capaian** | |
| Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, di dokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a) Kawalan capaian ke atas aset Jabatan/ Agensi mengikut keperluan keselamatan dan peranan pengguna;<br><br>b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;<br><br>c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan<br><br>d) Kawalan ke atas kemudahan pemprosesan maklumat. | **ICTSO**<br><br>**Pentadbir Sistem Aplikasi**<br><br>**Pentadbir Rangkaian** |
| **5.15.1.1: Capaian Rangkaian** | |
| Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:<br><br>a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian Jabatan/ Agensi, rangkaian agensi lain dan rangkaian awam; | **Pentadbir Rangkaian** |

| | |
|---|---|
| b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya;<br><br>c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; dan<br><br>d) Permohonan capaian perlu mendapat kebenaran pentadbir sistem dengan mendaftarkan keterangan komputer. | |
| **5.15.1.2: Capaian Internet** | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a) Penggunaan Internet di Jabatan/ Agensi hendaklah dipantau secara berterusan oleh pentadbir rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, *virus* dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian Jabatan/ Agensi ;<br><br>b) Kaedah *Content Filtering* boleh digunakan bagi mengawal akses internet mengikut fungsi kerja dan pemantauan tahap pematuhan;<br><br>c) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan;<br><br>d) Penggunaan internet hanyalah untuk kegunaan rasmi sahaja. Ketua Jabatan/ Agensi berhak menentukan pengguna yang dibenarkan menggunakan internet atau sebaliknya;<br><br>e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh pengarah/ pegawai yang diberi kuasa; | **Pentadbir Rangkaian** |

| | |
|---|---|
| f) Bahan yang diperoleh dari internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber internet hendaklah dinyatakan;<br><br>g) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan/ Agensi sebelum dimuat naik ke Internet;<br><br>h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;<br><br>i) Sebarang bahan yang dimuat turun dari sumber internet/ laman web yang selamat hendaklah digunakan untuk tujuan yang dibenarkan oleh Jabatan/ Agensi ;<br><br>j) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CDO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan;<br><br>k) Penggunaan *modem* atau '*broadband'* untuk tujuan sambungan ke internet tidak dibenarkan sama sekali; dan<br><br>l) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:<br><br>i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan<br><br>ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah. | |

| | |
|---|---|
| Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada *Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003* bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*". | |
| **5.15.2: Kawalan Capaian Sistem Pengoperasian** | |
| **5.15.2.1: Capaian Sistem Pengoperasian** | |
| Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi:-<br>a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan;<br>b) Merekodkan capaian yang berjaya dan gagal; dan<br>Kaedah-kaedah yang digunakan hendaklah Jabatan/ Agensi menyokong perkara-perkara berikut:-:<br>a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan;<br>b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user/super admin*;<br>c) Menjana amaran (*alert*) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem; dan<br>d) Menyediakan tempoh penggunaan mengikut kesesuaian.<br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:-:<br>a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; | **Pentadbir Pusat Data**<br>**Pegawai Aset ICT dan Pentadbir Teknikal** |

| | |
|---|---|
| b) Mewujudkan satu pengenalan diri (*ID*) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;<br>c) Menghadkan dan mengawal penggunaan program; dan<br>d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi. | |
| **5.15.2.2: Pas Keselamatan** | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br>a. Penggunaan pas keselamatan kakitangan hendaklah digunakan bagi memasuki premis Jabatan/ Agensi Kerajaan Negeri Melaka;<br>b. Pas Keselamatan hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain;<br>c. Pelawat perlu mendapatkan kad pelawat di pondok pengawal keselamatan untuk memasuki premis Jabatan/ Agensi Kerajaan Negeri Melaka; dan<br>d. Pas keselamatan hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain. | **Unit Khidmat Pengurusan** |
| **5.15.3: Kawalan Capaian Aplikasi Dan Maklumat** | |
| **5.15.3.1: Capaian Maklumat Dan Sistem Aplikasi** | |
| Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: | **Pentadbir Sistem Aplikasi** |

| | |
|---|---|
| a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;<br>b) Menghadkan capaian sistem dan aplikasi kepada minima tiga (3) kali percubaan adalah disyorkan. Sekiranya gagal, akaun atau kata laluan pengguna boleh disekat;<br>c) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan<br>d) Capaian sistem maklumat dan aplikasi melalui VPN bagi perkhidmatan yang terhad adalah digalakkan. | |
| **5.16: Pengurusan Identiti** | |
| **Objektif:**<br>Membenarkan individu dan sistem yang menggunakan identiti unik bagi membuat capaian kepada maklumat Jabatan/ Agensi dan aset ICT serta melaksanakan tugasan berdasarkan hak capaian. | |
| **5.16.1: Akaun Pengguna** | |
| Pengguna adalah bertanggungjawab ke atas aset ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah yang perlu dipatuhi adalah seperti berikut:-:<br>a) Pengguna perlu mendaftar akaun menggunakan Borang Permohonan/ Perubahan Sistem dan Operasi ICT (Borang C) atau setara;<br>b) Akaun yang diperuntukkan sahaja boleh digunakan;<br>c) Akaun pengguna (*user id*) hendaklah unik;<br>d) Pemilik akaun pengguna bukanlah hak mutlak pengguna dan ia tertakluk kepada peraturan. Akaun pengguna boleh | **Semua** |

| | |
|---|---|
| disekat dan ditarik balik jika pengguna melanggar peraturan yang ditetapkan;<br>e) Tidak semua pengguna boleh mencapai semua peringkat maklumat. Terdapat peringkat-peringkat di dalam capaian maklumat dan ditentukan oleh Pentadbir Sistem Aplikasi. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;<br>f) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;<br>g) Akaun pengguna boleh dibekukan dan ditamatkan atas sebab-sebab berikut:-:<br>i. Cuti belajar;<br>ii. Bertukar bidang tugas kerja;<br>iii. Bertukar ke agensi lain;<br>iv. Bersara;<br>v. Digantung perkhidmatan; atau<br>vi. Ditamatkan perkhidmatan<br>h) Penamatan akaun hendaklah menggunakan Borang Penamatan Akaun Aplikasi dan Pemulangan Peralatan ICT (Borang J) atau setara;<br>i) Bahagian ICT di Jabatan/ Agensi perlu mengambil tindakan sewajarnya dalam tempoh 14 hari dari tarikh akhir pegawai/ kakitangan berkhidmat; dan<br>j) Kata laluan bagi pengguna berkenaan hendaklah diubah selepas tarikh perpindahan atau persaraan kakitangan berkenaan atau ID pengguna digantung dalam tempoh tiga (3) bulan sebelum dimansuhkan. | |

| 5.17: Maklumat Pengesahan | |
|---|---|
| **Objektif:**<br>Memastikan pengesahan entiti yang betul dan mencegah kegagalan proses pengesahan. | |
| **5.17.1: Pengurusan Katalaluan** | |
| Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan seperti berikut:<br>a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;<br>b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;<br>c) Pengguna tidak digalakkan untuk menggunakan kemudahan pengurus kata laluan pelayar seperti *google chrome, Mozilla Firefox* dan seumpamanya bagi mengelakkan risiko penyalahgunaan capaian;<br>d) Panjang kata laluan disyorkan sekurang-kurangnya 12 aksara dengan gabungan huruf besar, huruf kecil, angka dan aksara khas;<br>e) Parameter katalaluan;<br>f) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun;<br>g) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain;<br>h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;<br>i) Pengguna digalakkan menukar kata laluan setiap enam (6) bulan atau selepas tempoh masa yang bersesuaian; | **Pemilik Sistem Aplikasi** |

| | |
|---|---|
| j) Senarai kata laluan *root* bagi server dan *appliance* serta kata laluan Administrator Komputer akan diberikan kepada ICTSO serta disahkan dan disimpan di dalam kabinet berkunci setiap enam (6) bulan sekali; dan<br>k) ICTSO perlu mengesahkan penerimaan senarai kata laluan tersebut menggunakan buku log simpanan kata laluan. | |
| **5.18: Hak Capaian** | |
| **Objektif:**<br>Memastikan capaian kepada maklumat dan aset lain yang berkaitan ditakrifkan dan dibenarkan mengikut keperluan organisasi. | |
| **5.18.1: Semakan Hak Capaian Pengguna** | |
| Penetapan dan penggunaan ke atas hak capaian perlu disemak dari semasa ke semasa, diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas bagi memastikan tiada berlaku penyalahgunaan hak capaian. | **Unit Teknologi Maklumat** |
| **5.18.2: Pembatalan Atau Kemas Kini Hak Capaian** | |
| Perkara yang perlu dipatuhi adalah seperti berikut:<br>a) Hak capaian pengguna untuk kemudahan pemprosesan data dan maklumat hendaklah dibatalkan selepas tamat perkhidmatan, kontrak atau perjanjian;<br>b) Kemas kini hak capaian pengguna perlulah dilakukan apabila berlaku perubahan dalaman atau perubahan bidang tugas;<br>c) Kemas kini hak capaian pengguna menggunakan Borang Permohonan/ Perubahan Sistem dan Operasi ICT (Borang C) atau setara; dan | **Unit Teknologi Maklumat** |

| | |
|---|---|
| d) Penamatan hak capaian hendaklah menggunakan Borang Penamatan Akaun Aplikasi dan Pemulangan Peralatan ICT (Borang J) atau setara. | |
| **5.19: Hubungan Keselamatan Maklumat Dengan Pembekal** | |
| **Objektif:**<br>Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dengan pembekal. | |
| Keperluan keselamatan maklumat dengan pembekal hendaklah dipersetujui dan didokumentasikan bagi mengurangkan risiko kepada aset Jabatan/ Agensi .<br><br>Perkara-perkara lain yang perlu diteliti dan dipatuhi seperti berikut:<br><br>a) Mengawal dan memantau akses pembekal;<br><br>b) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian;<br><br>c) Jenis-jenis obligasi kepada pembekal;<br><br>d) Pelan kontigensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat;<br><br>e) Melaksanakan program kesedaran terhadap Polisi Keselamatan Siber Jabatan/ Agensi kepada pembekal;<br><br>f) Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber dan Sistem Pengurusan Keselamatan Maklumat (ISMS) (**LAMPIRAN 2**); dan<br><br>g) Pembekal perlu mematuhi arahan keselamatan yang berkuatkuasa. | **Semua** |

| 5.20: Perjanjian Keselamatan Maklumat Dengan Pembekal | |
|---|---|
| **Objektif:**<br>Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dengan pembekal. | |
| Semua keperluan keselamatan maklumat hendaklah relevan dan dipersetujui dengan setiap pembekal bagi mengakses, memproses,menyimpan, berkomunikasi atau menyediakan komponen infrastruktur dan maklumat organisasi ICT.<br><br>Perkara-perkara yang perlu diambil kira adalah seperti berikut:<br><br>a) Penerangan maklumat keselamatan;<br>b) Klasifikasi maklumat;<br>c) Keperluan undang-undang dan peraturan;<br>d) Obligasi setiap pihak bagi kawalan akses, pemantauan, pelaporan dan pengauditan;<br>e) Penerimaan peraturan penggunaan maklumat oleh pembekal;<br>f) Kesedaran keselamatan maklumat;<br>g) Tapisan keselamatan pembekal;<br>h) Hak untuk mengaudit pembekal;<br>i) Kewajipan pembekal mematuhi keperluan keselamatan maklumat; dan<br>j) Menandatangani *Non-Disclosure Agreement* (NDA). | **Jabatan/ Agensi Pembekal** |

| **5.21: Pengurusan Keselamatan Maklumat Dalam Rantaian Komunikasi Maklumat ICT** | |
|---|---|
| **Objektif:**<br>Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dengan pembekal. | |
| Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk.<br>Perkara-perkara lain yang perlu diteliti dan dipatuhi seperti berikut:<br>a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan;<br>b) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan<br>c) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik. | **Jabatan/ Agensi Pembekal** |

| **5.22: Pemantauan, Semakan Dan Perubahan Pengurusan Perkhidmatan Pembekal** | |
|---|---|
| **Objektif:**<br>Untuk mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal. | |
| Jabatan/ Agensi hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala.<br>Perkara-perkara yang perlu diteliti dan dipatuhi seperti berikut: | **Jabatan/ Agensi Pembekal** |

| | |
|---|---|
| a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan;<br>b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan<br>c) Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.<br><br>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.<br><br>Perkara-perkara lain yang perlu diteliti dan dipatuhi seperti berikut:<br>a) Perubahan dalam perjanjian dengan pembekal;<br>b) Perubahan yang dilakukan oleh Jabatan/ Agensi bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan<br>c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan subkontraktor. | |
| **5.23: Keselamatan Maklumat Bagi Penggunaan Perkhidmatan Awan** | |
| **Objektif:**<br><br>Untuk menentukan dan mengurus keselamatan maklumat untuk penggunaan perkhidmatan awan. | |

| | |
|---|---|
| Perkhidmatan awan adalah penting untuk memastikan bahawa organisasi memilih penyedia perkhidmatan awan yang mempunyai tahap keselamatan yang tinggi.<br><br>Walaupun terdapat kepentingan dalam menggunakan perkhidmatan awan, konfigurasi yang salah dan pengurusan yang tidak cekap boleh menjejaskan perkhidmatan. Kawalan ini menekankan penyediaan proses yang lebih baik untuk mengakses, menggunakan, mengekalkan, dan keluar dari infrastruktur awan. | |
| "Kerajaan Negeri Melaka menggunapakai rangka kerja dan dokumen Cloud Framework Agreement (CFA) yang dibangunkan oleh Jabatan Digital Negara (JDN) sebagai garis panduan rujukan utama dalam pelaksanaan, pemantauan dan penambahbaikan keseluruhan tahap keselamatan siber di semua agensi Kerajaan Negeri. Cloud Framework Agreement (CFA) merupakan dokumen kontrak antara Kerajaan melalui JDN dengan Cloud Service Provider (CSP) dan Managed Service Provider (MSP) yang dilantik oleh Kerajaan bagi menyediakan perkhidmatan cloud kepada semua Agensi Kerajaan. | **Jabatan/ Agensi** |
| **5.24: Perancangan, Penyediaan Dan Pengurusan Insiden Keselamatan Maklumat** | |
| **Objektif:**<br><br>Memastikan insiden keselamatan siber dan kelemahan dilapor dan disalur dengan cepat dan berkesan bagi meminimumkan proses pembaikan dan mengurangkan kesan insiden keselamatan siber. | |
| Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada Jabatan/ Agensi . | **ICTSO**<br><br>**Pentadbir Keselamatan dan Rangkaian** |

| | |
|---|---|
| Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan diselenggarakan. Tindakan menangani insiden keselamatan ICT perlu dilakukan dengan cepat, teratur dan berkesan.<br><br>Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:-:<br><br>a) Mengenal pasti jenis insiden keselamatan ICT;<br>b) Menyimpan jejak audit, sandaran (*backup*) secara berkala dan melindungi integriti semua bahan bukti;<br>c) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;<br>d) Menyediakan, melaksanakan dan menyelenggara Pelan Kesinambungan Perkhidmatan dan mengaktifkan pelan tersebut;<br>e) Menyediakan tindakan pemulihan dan pengukuhan dengan segera;<br>f) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu;<br>g) Memberikan kesedaran berkaitan Prosedur Pengurusan Insiden Keselamatan ICT dan hebahan kepada warga Jabatan/ Agensi sekiranya terdapat pindaan; dan<br>h) Memastikan pegawai bertanggungjawab menguruskan insiden mempunyai tahap kompetensi yang diperlukan. | |

**5.25: Penilaian Dan Keputusan Peristiwa Keselamatan Maklumat**

**Objektif:**

Memastikan insiden keselamatan ICT dan kelemahan dilapor dan disalur dengan cepat dan berkesan bagi meminimumkan proses pembaikan dan mengurangkan kesan insiden keselamatan ICT.

| | |
|---|---|
| Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat. Penilaian ini bertujuan untuk memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT Jabatan/ Agensi. Jenis situasi insiden yang terlibat adalah:<br>a. Maklumat didapati hilang atau disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;<br>b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;<br>c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang;<br>d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan<br>e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. | **ICTSO**<br><br>**Pasukan CSIRT** |
| **5.26: Maklumbalas Insiden Keselamatan Maklumat** | |
| **Objektif:**<br>Memastikan tindakan terhadap insiden keselamatan ICT dapat dilaksanakan dengan cepat dan berkesan. | |
| Insiden keselamatan maklumat hendaklah ditangani berdasarkan prosedur pengurusan insiden keselamatan ICT yang didokumenkan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut:<br>a) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku;<br>b) Menjalankan kajian forensik sekiranya perlu; | **ICTSO**<br><br>**Pasukan CSIRT** |

| | |
|---|---|
| c) Menghubungi pihak yang berkenaan dengan secepat mungkin;<br>d) Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti;<br>e) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;<br>f) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan;<br>g) Menyediakan tindakan pemulihan dan pengukuhan dengan segera; dan<br>h) Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu. | |
| **5.27: Pembelajaran Daripada Insiden Keselamatan Maklumat** | |
| Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada Jabatan/ Agensi Negeri. | **ICTSO**<br><br>**Pasukan CSIRT** |
| **5.28: Pengumpulan Bukti** | |
| **Objektif:**<br>Memastikan bukti insiden keselamatan ICT dapat direkod dan dianalisa bagi tujuan kegunaan pengesahan tindakan displin dan undang-undang. | |
| Jabatan/ Agensi hendaklah mengenal pasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan. | **ICTSO** |

| | |
|---|---|
| Memastikan pengurusan bukti yang konsisten dan berkesan berkaitan insiden ICT untuk tujuan tindakan tatatertib dan undang-undang.<br>Bukti sepatutnya boleh ditunjukkan bahawa;<br>a. Rekod adalah lengkap dan tidak diusik dengan apa cara sekalipun;<br>b. salinan bukti elektronik mungkin sama dengan yang asal; dan<br>c. mana-mana sistem maklumat yang mana bukti telah dikumpulkan telah beroperasi dengan betul pada masa bukti direkodkan. | |
| **5.29: Keselamatan Maklumat Semasa Gangguan** | |
| **Objektif:**<br>Memastikan maklumat dan aset berkaitan dalam keadaan selamat. | |
| **5.29.1: Pelan Kesinambungan Perkhidmatan** | |
| Pelan Kesinambungan Perkhidmatan (PKP) menyediakan kerangka pengurusan (*management framework*) untuk memulihkan perkhidmatan secara formal supaya Jabatan/ Agensi dapat meneruskan operasi sekiranya berlaku gangguan ICT. PKP hendaklah diurus dan dirangka dengan tepat dengan perbelanjaan yang berpatutan. | **Bahagian Khidmat Pengurusan** |
| **5.29.2: *Backup* dan *Restore*** | |
| Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah mengikut prosedur yang telah ditetapkan.<br>Perkara-perkara yang perlu dicontohi adalah seperti berikut : | **Pentadbir Pusat Data** |

| | |
|---|---|
| a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; dan<br>b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi.<br>c) Menguji sistem *backup* dan *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan sekurang-kurangnya dua (2) kali setahun;<br>d) Melaksanakan *backup* mengikut jadual yang ditetapkan;dan<br>e) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat. | |
| **5.30: Ketersediaan ICT Untuk Kesinambungan Perkhidmatan** | |
| **Objektif:**<br>Memastikan maklumat dan aset berkaitan dalam keadaan selamat. | |
| Teknologi Maklumat dan Komunikasi (ICT) adalah aspek penting dalam memastikan kesinambungan perkhidmatan organisasi. Ini melibatkan penyediaan infrastruktur, sistem dan perkhidmatan ICT yang boleh diakses dan berfungsi dengan baik dalam semua keadaan, termasuk semasa krisis atau gangguan. Faktor-faktor yang perlu dipertimbangkan untuk mencapai ketersediaan ICT bagi kesinambungan perkhidmatan adalah seperti berikut:<br>a. Organisasi perlu mempunyai perancangan strategik ICT yang jelas dan menyeluruh yang mengenal pasti keperluan teknologi bagi menjayakan strategi kesinambungan perkhidmatan; | **Unit Teknologi Maklumat** |

| | |
|---|---|
| b. Ini termasuk menentukan sumber daya ICT yang diperlukan, tujuan pemulihan dan proses perolehan peralatan dan perkhidmatan yang cekap;<br>c. Mempunyai infrastruktur ICT yang *redundant*, termasuk rangkaian, pelayan, storan data, dan sokongan kuasa yang boleh berfungsi jika ada gangguan atau kegagalan;<br>d. Penggantian secara automatik *(failover)* dan peralatan cadangan perlu dipertimbangkan;<br>e. Lakukan pemantauan terhadap peralatan ICT untuk mengenalpasti masalah sebelum ia berlaku dan mengelakkan gangguan;<br>f. Pengurusan inventori peralatan, pelan pembaikan, dan pemantauan prestasi berterusan.<br>Sediakan pelan pemulihan bencana ICT yang komprehensif, merangkumi;<br>a. Pelan Pemulihan Bencana ICT (ICT DRP) perlu dirangka dan diuji kesesuaian dan ketepatannya dari semasa ke semasa;<br>b. ICT DRP perlu dikemas kini dari semasa ke semasa dan diedarkan kepada semua yang berkaitan;<br>c. Pihak yang terlibat hendaklah melaksanakan bidang tugas masing-masing apabila berlaku gangguan perkhidmatan yang memerlukan ICT DRP diaktifkan;<br>d. Ujian pemulihan ICT atau simulasi hendaklah dilakukan mengikut ketetapan pengurusan; dan<br>e. Hasil ujian untuk analisa dan rancangan pembetulan prosedur hendaklah didokumenkan. | |

| **5.31: Pematuhan Terhadap Keperluan Perundangan, pekeliling, Peraturan Dan Perjanjian Kontrak** | |
|---|---|
| **Objektif:**<br><br>Meningkat dan memantapkan tahap keselamatan siber bagi mengelak daripada pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat. | |
| Faktor perundangan hendaklah dikenalpasti dan semua kakitangan terlibat wajib mematuhinya, pihak syarikat pembekal, pakar-pakar runding dan mana-mana pihak yang berurusan dengan pihak Jabatan/ Agensi juga perlu mematuhi undang-undang dan peraturan yang diterima pakai. Senarai perundangan dan peraturan yang perlu dipatuhi adalah seperti di **LAMPIRAN 1**. Perkara berkaitan perundangan yang perlu diberi perhatian adalah seperti berikut:<br><br>a) Setiap pengguna hendaklah membaca, memahami dan mematuhi PKS Jabatan/ Agensi dan undang-undang atau peraturan-peraturan lain berkaitan yang berkuatkuasa;<br><br>b) Semua perjanjian dan pekeliling berkaitan ICT termasuk maklumat yang disimpan di dalamnya adalah hakmilik Jabatan/ Agensi dan Ketua Jabatan berhak memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan;<br><br>c) Sebarang penggunaan aset Jabatan/ Agensi selain daripada maksud dan tujuan yang telah ditetapkan adalah merupakan satu penyalahgunaan sumber Jabatan/ Agensi. | **Semua** |

| 5.32: Hak Harta Intelek | |
|---|---|
| Hak Harta Intelek Jabatan/ Agensi perlu dilindungi melalui penguatkuasaan perundangan dan peraturan yang telah ditetapkan. Data-data dan dokumen yang digunapakai perlu dipastikan asli dan tidak diambil daripada harta intelek pihak lain. Semua aplikasi yang digunakan hendaklah yang asli (*genuine*). | **Semua** |
| **5.33: Perlindungan Rekod** | |
| **Objektif:**<br>Memastikan pematuhan kepada keperluan undang-undang, berkanun, peraturan dan kontrak, serta jangkaan komuniti atau masyarakat yang berkaitan dengan perlindungan dan ketersediaan rekod. | |
| 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 seperti Akta Arkib Negara, Arahan Keselamatan dan Garis Panduan Keselamatan Maklumat Terbitan 2023. | **Semua** |
| **5.34: Privasi Dan Perlindungan Maklumat Pengenalan Peribadi** | |
| **Objektif:**<br>Memberikan jaminan dalam melindungi maklumat peribadi pengguna. | |
| Maklumat peribadi pengguna hendaklah dilindungi sebaiknya oleh pihak Jabatan/ Agensi. Kawalan yang ketat perlu dilaksanakan agar maklumat tidak mudah diberikan kepada pihak lain mengikut perundangan dan peraturan yang ditetapkan seperti yang dinyatakan di dalam Panduan Data Peribadi Sektor Awam yang terkini. | **Semua** |

| 5.35: Semakan Semula Keselamatan Maklumat | |
|---|---|
| **Objektif:**<br>Mengkaji kesesuaian, kecukupan dan keberkesanan pengurusan keselamatan maklumat organisasi. | |
| Penilaian keselamatan maklumat oleh organisasi hendaklah dilaksanakan secara berkala seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur melalui audit dalaman dan luaran. | **Semua** |
| **5.36: Pematuhan Polisi, Peraturan Dan Piawaian Keselamatan Maklumat** | |
| **Objektif:**<br>Memastikan pengurusan keselamatan maklumat organisasi adalah berdasarkan kepada polisi, peraturan dan standard yang ditetapkan. | |
| Memastikan semua warga Jabatan/ Agensi dan pihak ketiga yang berkaitan mematuhi semua polisi, peraturan dan piawaian keselamatan maklumat yang ditetapkan. Sebarang ketidakpatuhan polisi, peraturan dan piawaian keselamatan maklumat tindakan tatatertib boleh diambil mengikut kesalahan. | **Semua** |
| **5.37: Prosedur Operasi Yang Didokumen** | |
| **Objektif:**<br>Memastikan prosedur operasi diwujudkan dan didokumentasikan. | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut :<br>a) Semua prosedur keselamatan siber yang diwujudkan, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal;<br>b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian serta pemprosesan maklumat, pengendalian serta penghantaran ralat, pengendalian output, bantuan | **Semua** |

| | |
|---|---|
| teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan<br>c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan. | |

| PERKARA | PERANAN |
|---|---|
| **BIDANG 6 – KAWALAN MANUSIA** | |
| Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan, pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa. | |
| **6.1: Saringan** | |
| a. Pihak pengurusan hendaklah memastikan pegawai dan kakitangan menjalani tapisan keselamatan, khususnya bagi mereka yang mengendalikan maklumat berperingkat, berasaskan keperluan perundangan, peraturan, etika yang terpakai serta selaras dengan keperluan perkhidmatan, tahap maklumat yang akan diakses dan risiko yang dijangka, sebagaimana yang diperuntukkan dalam Arahan Keselamatan (Semakan & Pindaan 2017); dan | **Pengurusan Sumber Manusia** |
| b. Peranan dan tanggungjawab pegawai serta kakitangan Jabatan/ Agensi yang terlibat dalam memastikan keselamatan aset ICT hendaklah dinyatakan secara terperinci dan jelas, termasuk tanggungjawab mereka dalam pelaksanaan kawalan keselamatan sebelum akses diberikan, semasa pengendalian maklumat, dan selepas tamat perkhidmatan. Ini bertujuan memastikan keselamatan maklumat terpelihara, mencegah kebocoran data, serta menguruskan aset dengan baik selepas digunakan, selaras dengan garis panduan dan prosedur yang ditetapkan. | **Pengurusan Sumber Manusia**<br>**Unit Teknologi Maklumat** |

| 6.2: Terma Dan Syarat Pekerjaan | |
|---|---|
| Memastikan semua pihak memahami tanggungjawab ke atas keselamatan maklumat berdasarkan peranan mereka di organisasi.<br>Perkara-perkara yang perlu dipatuhi termasuk yang berikut:-<br>a) Memastikan pegawai dan kakitangan serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh Jabatan/ Agensi; | **Pengurusan Sumber Manusia** |
| b) Kakitangan yang dilantik diberi surat tawaran dan perjanjian (kakitangan kontrak) yang menerangkan peraturan-peraturan dan syarat-syarat Jabatan/ Agensi dan Kerajaan dari semasa ke semasa; | **BTMK** |
| c) Kakitangan tetap yang baru dilantik perlu menandatangani dan sertakan :<br>i) Borang Pengesahan Melapor Diri<br>ii) Borang Data Peribadi<br>iii) Surat Aku Janji (Alamat Jabatan)<br>iv) Borang Akta Rahsia 1972<br>v) Salinan Kad Pengenalan<br>vi) Salinan Akaun Bank<br>vii) Salinan Penyata KWSP<br>viii)Penyata Kew.8 (Jabatan Negeri sahaja)<br>ix) Borang Akuan Pematuhan Polisi Keselamatan Siber<br>x) Borang Akuan Berkanun (dari SPA)<br>xi) Borang Setuju Terima Pelantikan (dari SPA)<br>xii) Salinan Permohonan e-Vetting<br>d) Kakitangan kontrak yang baru dilantik perlu menandatangani dan sertakan :<br>i) Borang Pengesahan Melapor Diri<br>ii) Borang Data Peribadi | **Pengurusan Sumber Manusia** |

| | |
|---|---|
| iii) Borang Perjanjian Kontrak (Interim)<br>iv) Surat Aku Janji (Alamat Jabatan)<br>v) Borang Akta Rahsia 1972<br>vi) Salinan Kad Pengenalan<br>vii) Salinan Akaun Bank<br>viii) Salinan Penyata KWSP<br>ix) Penyata Kew.8 (Jabatan Negeri sahaja)<br>x) Borang Akuan Pematuhan Keselamatan Siber<br>xi) Borang Akuan Berkanun (dari SPA)<br>xii) Borang Setuju Terima Pelantikan (dari SPA)<br>xiii) Salinan Permohonan e-Vetting | |
| **6.3: Kesedaran Keselamatan Maklumat, Pendidikan Dan Latihan** | |
| a. Setiap pengguna perlu diberikan program kesedaran, latihan atau sebarang medium penyampaian yang bersesuaian mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden keselamatan ICT juga adalah penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT di Jabatan/ Agensi;<br>b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT Jabatan/ Agensi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari masa ke semasa; dan<br>c. Setiap lantikan kakitangan baru akan diberi taklimat berkaitan polisi keselamatan siber. Manakala bagi kakitangan sedia ada, Unit Latihan Jabatan/ Agensi masing-masing akan merancang untuk membuat kesedaran ICT melalui sebarang medium yang bersesuaian. | **<u>INDUK</u>**<br>**BPSM**<br><br>**<u>AHLI</u>**<br>**BTMK** |

| 6.4: Proses Tindakan Tatatertib | |
|---|---|
| Proses tindakan disiplin dan atau undang-undang ke atas pegawai dan kakitangan serta pihak ketiga yang berkepentingan perlu diambil sekiranya berlaku pelanggaran dengan perundangan dan peraturan yang ditetapkan.<br><br>Prosedur proses tindakan tatatertib telah diwujudkan yang melibatkan beberapa langkah utama yang mana boleh dirujuk adalah seperti yang berikut:<br><br>**a) Peringatan dan Hebahan Tatatertib Penjawat Awam**<br><br>Unit Integriti terlibat secara langsung di dalam menyebarkan mesej-mesej peringatan dan hebahan tatatertib yang dilaksanakan secara berkala melalui platform-platform sosial media rasmi negeri ataupun media-media arus perdana selainnya. Modus operandi pelaksanaan hebahan ini adalah melalui kolaborasi bersama jabatan/ agensi berkaitan seperti Bahagian Komunikasi Korporat atau Jabatan Penerangan Malaysia ataupun agensi-agensi lain yang berkepentingan bagi menyalurkan informasi berkaitan kesedaran amalan integriti dalam perkhidmatan awam.<br><br>**b) Pembangunan Dasar:**<br><br>Unit Integriti, Jabatan Ketua Menteri Melaka adalah terikat kepada peraturan-peraturan dan dasar-dasar yang sedang berkuatkuasa berhubung kelakuan, tatatertib dan Lembaga Tatatertib sama ada di peringkat persekutuan ataupun di peringkat Kerajaan Negeri iaitu peraturan yang terpakai terhadap penjawat awam lantikan persekutuan yang berkhidmat di Negeri Melaka ataupun penjawat-penjawat awam di negeri sama ada berstatus lantikan tetap ataupun lantikan kontrak. | **Unit Integriti** |

| | |
|---|---|
| **c) Dokumentasi:**<br><br>Urusan dokumentasi berkaitan tindakan tatatertib penjawat awam di Negeri Melaka dan urusan pembentukan Lembaga Tatatertib adalah berdasarkan kepada Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib)(Negeri Melaka)(Pindaan) 2003 dan Peraturan-Peraturan Lembaga Tatatertib Perkhidmatan Awam Negeri Melaka 2005.<br><br>**d) Penyiasatan:**<br><br>Prosedur untuk menyiasat insiden yang dilaporkan adalah dengan menubuhkan jawatankuasa siasatan yang keanggotaannya dilantik oleh pengerusi lembaga tatatertib. Jawatankuasa siasatan ini akan mengadakan mesyuarat, temu bual saksi, mengumpul bukti, dan mendokumentasikan penemuan secara berekod iaitu yang dikenali sebagai laporan rasmi/penuh jawatankuasa siasatan bagi rujukan lembaga tatatertib yang akan bersidang kemudiannya.<br><br>e) **Keadilan:**<br><br>Unit Integriti sentiasa menitikberatkan konsep professioanlisme, keadilan dan konsistensi sepanjang proses tindakan tatatertib berlangsung. Proses kerja bagi isu-isu tatatertib yang berbangkit sentiasa dipatuhi sewajarnya bermula daripada aduan yang diterima sehingga kepada keputusan lembaga tatatertib. | |
| **6.5: Tanggungjawab Selepas Penamatan Atau Perubahan Pekerjaan** | |
| Perkara-perkara yang perlu dipatuhi termasuk yang berikut:<br><br>a) Memastikan semua aset ICT dikembalikan kepada Jabatan/ Agensi mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan;<br><br>b) Penamatan Perkhidmatan/ Peletakan Jawatan; | **Pegawai Aset** |

| | |
|---|---|
| i. Surat Akuan Penerimaan notis perletakan jawatan diterima daripada pegawai/ kakitangan dan disertakan bersekali dengan Pas Keselamatan;<br><br>ii. Borang Perakuan apabila meninggalkan perkhidmatan Awam (perlu diisi sekiranya mendapatkan tawaran selain agensi Kerajaan); | **Pengurusan Sumber Manusia** |
| iii. Membatalkan atau menarik balik semua kebenaran capaian keatas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh Jabatan/ Agensi dan /atau terma perkhidmatan; dan<br><br>iv. Bertanggungjawab menguruskan segala tanggungan hutang dengan Jabatan/ Agensi dan Kerajaan. | **Unit Teknologi Maklumat** |
| c) Persaraan Wajib/ Paksa<br>i. Mengemukakan memo penamatan pas keselamatan bakal pesara kepada Bahagian Khidmat Pengurusan;<br>ii. Memastikan bakal pesara menandatangani Perakuan Meninggalkan Perkhidmatan Kerajaan Berkaitan Dengan Akta Rahsia Rasmi 1972 (Akta 88);<br>iii. Mengemukakan surat pengesahan akuan berhutang bakal pesara kepada Jabatan Kewangan dan Perbendaharaan Negeri Melaka; dan | **Pengurusan Sumber Manusia** |
| iv. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh Jabatan/ Agensi dan /atau terma perkhidmatan dengan mengisi Borang J (Borang Penamatan Akauan Aplikasi dan Pemulangan Peralatan). | **Unit Teknologi Maklumat** |

| 6.6: Kerahsiaan Atau Perjanjian *Non-Disclosure* | |
|---|---|
| Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan Jabatan/ Agensi dan hendaklah disemak dan didokumentasikan. | **Pengurusan Sumber Manusia** |
| Jabatan/ Agensi/ Pembekal/ pihak luaran/ pihak ketiga hendaklah bersetuju dan menandatangani satu dokumen Aku Janji untuk mematuhi semua keperluan keselamatan maklumat yang relevan. | **Jabatan/ agensi/ Pembekal/pihak luaran/pihak ketiga** |
| **6.7: Bekerja Luar Pejabat** | |
| Memastikan keselamatan maklumat terjamin apabila terdapat kakitangan bekerja dari luar pejabat yang memerlukan capaian jarak jauh.<br><br>Perkara-perkara yang perlu dipatuhi termasuk yang berikut:<br><br>i. **Dasar dan Garis Panduan:**<br><br>Dasar Bekerja Dari Rumah (BDR) diperuntukkan melalui Pekeliling Perkhidmatan Sumber Manusia (MyPPSM) Ceraian SR.4.1.2: Dasar Bekerja Dari Rumah bagi pegawai Perkhidmatan Awam Persekutuan berkuat kuasa mulai 1 Januari 2021. | **Pengurusan Sumber Manusia** |
| ii. **Kaedah Pelaksanaan**<br>a) Pengisian Borang Lembaran Sr.4.1.2(A) Arahan Bekerja Dari Rumah (BDR); dan<br>b) Pengisian Borang Lembaran Sr.4.1.2(B) Permohonan Bekerja Dari Rumah (BDR).<br><br>iii. **Fleksibiliti dan Waktu Bekerja**<br><br>Pegawai yang melaksanakan tugasan secara Bekerja Dari Rumah (BDR) hendaklah mematuhi waktu bekerja rasmi selaras dengan jadual atau skim perkhidmatan masing-masing, sama ada:<br>a) Waktu Bekerja Pejabat, | **Unit Teknologi Maklumat** |

| | |
|---|---|
| b) waktu Bekerja Bukan Pejabat, atau<br>c) waktu Bekerja Fleksi yang ditetapkan oleh jabatan.<br>Bagi pegawai yang telah mendapat kelulusan untuk BDR, kehadiran harian hendaklah direkodkan secara manual atau mengikut tatacara Jabatan/ Agensi masing-masing.<br><br>iv. **Tempat Bekerja**<br>Tempat bekerja pegawai semasa BDR ialah rumah. Rumah adalah kediaman pegawai seperti alamat tempat tinggal yang didaftarkan dalam Sistem Pengurusan Maklumat Sumber Manusia (HRMIS) atau lokasi yang bersesuaian sebagai tempat bekerja tertakluk kepada pertimbangan dan kelulusan Ketua Jabatan. | **Bahagian/Unit Teknologi Maklumat** |
| v. **Teknologi dan Infrastruktur:**<br>Memastikan setiap pegawai mempunyai akses yang mencukupi dan selamat kepada teknologi yang diperlukan seperti komputer, perisian pejabat, sambungan internet berkelajuan tinggi, serta perkhidmatan keselamatan rangkaian seperti Virtual Private Network (VPN) yang menyokong *end-to-end encryption, multifactor authentication* (MFA/2FA) sekiranya perlu; dan memastikan semua peranti dilengkapi dengan perisian keselamatan seperti *Endpoint Detection and Response* (EDR) atau sekurang-kurangnya perisian *antivirus* yang mampu mengesan *malware* dan *ransomwar*e secara *real-time*.<br><br>vi. **Komunikasi Berkesan:**<br>Memastikan semua transaksi, komunikasi, dan perkongsian data dilaksanakan melalui platform digital yang selamat, diluluskan, dan diselia oleh jabatan. Ini termasuk penggunaan e-mel rasmi jabatan, aplikasi persidangan video seperti Google Meet dan setara dengannya, serta storan awan rasmi seperti Melaka | **Unit Teknologi Maklumat** |

| | |
|---|---|
| Drive bagi tujuan penyimpanan dan perkongsian maklumat.<br><br>vii. **Pengurusan Keselamatan Maklumat:**<br><br>Memastikan keselamatan maklumat, sistem dan peralatan ICT semasa pelaksanaan tugasan Bekerja Dari Rumah (BDR) melalui penyediaan dan penguatkuasaan Prosedur Operasi Standard (SOP) berdasarkan:<br>a) Polisi Keselamatan Siber (PKS); dan<br>b) Rangka Kerja Keselamatan Sektor Awam (RAKKSSA).<br><br>Tanggungjawab pegawai merangkumi:<br><br>a) Menjamin kerahsiaan, integriti dan ketersediaan maklumat serta peralatan jabatan;<br>b) Mengakses data dan sistem mengikut skop tugas dan kelulusan yang ditetapkan; dan<br>c) Mematuhi kawalan keselamatan siber seperti kawalan akses berperingkat (*role-based access control*), pengesahan identiti (*secure authentication*), dan penggunaan log audit bagi pemantauan. | **Unit Teknologi Maklumat** |
| **6.8: Pelaporan Keselamatan Maklumat** | |
| Insiden keselamatan siber seperti berikut hendaklah dilaporkan dengan kadar segera:<br>a. Maklumat didapati hilang atau didedahkan kepada pihak yang tidak diberi kuasa atau disyaki hilang atau didedahkan kepada pihak yang tidak diberi kuasa;<br>b. sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;<br>c. kata laluan atau mekanisme kawalan akses hilang,<br>d. dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; | **ICTSO** |

| | |
|---|---|
| e. berlaku kejadian sistem yang luar biasa seperti<br>f. kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan<br>g. berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. | |

| PERKARA | PERANAN |
|---|---|
| **BIDANG 7 – KAWALAN FIZIKAL** | |
| **7.1: Perimeter Keselamatan Fizikal** | |
| **Objektif:**<br>Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman dan kerosakan. | |
| Kawalan fizikal kawasan adalah bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi dengan mengesan dan mencegah cubaan menceroboh. Kompleks Seri Negeri juga telah diwartakan sebagai Kawasan Larangan di bawah Akta Kawasan Larangan & Tempat Larangan 1959 pada 12 Disember 2019.<br>Antara langkah-langkah keselamatan fizikal adalah :-:<br>a) Lokasi hendaklah dikenal pasti dengan jelas;<br>b) lokasi hendaklah diperkukuhkan dengan keselamatan perimeter (halangan seperti dinding, siling, tingkap dan pintu) serta dikunci untuk mengawal kemasukan;<br>c) memasang alat penggera atau sistem keselamatan kamera litar tertutup;<br>d) menghadkan jalan keluar masuk menggunakan pas keselamatan atau pas pelawat;<br>e) mengadakan pondok kawalan oleh pengawal keselamatan;<br>f) menyediakan tempat atau bilik khas untuk pelawat-pelawat;<br>g) mewujudkan perkhidmatan kawalan keselamatan;<br>h) melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; | **Unit Khidmat Pengurusan** |

| | |
|---|---|
| i) merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan tempat-tempat yang memerlukan kawalan;<br>j) merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan khianat;<br>k) memastikan pembekal atau pelawat yang dibawa masuk mesti diiringi oleh pegawai yang bertanggungjawab sepanjang tempoh di lokasi berkaitan; dan<br>l) memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya. | |
| **7.2: Kemasukan Fizikal** | |
| **Objektif:**<br>Melindungi premis dan aset ICT daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan. | |
| **7.2.1: Kawalan Masuk Fizikal** | |
| Perkara-perkara yang perlu dipatuhi termasuk yang berikut:-:<br>a) Setiap warga kerja Jabatan/ Agensi hendaklah memakai atau mengenakan serta mempamerkan pas keselamatan sepanjang waktu bertugas;<br>b) setiap pelawat hendaklah mendaftar dan mendapatkan pas pelawat di pondok pengawal keselamatan dan pas dikembalikan semula selepas selesai urusan;<br>c) semua pas keselamatan hendaklah diserahkan balik kepada Unit Khidmat Pengurusan apabila kakitangan berhenti atau bersara;<br>d) kehilangan pas mestilah dilaporkan dengan segera; dan<br>e) semua kawasan larangan dipasang terminal akses kad. | **Semua Bahagian Khidmat Pengurusan** |

| | |
|---|---|
| **7.2.2: Keselamatan Persekitaran** | |
| Melindungi aset Jabatan/ Agensi dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan. | **Semua** |
| **7.2.3: Kawalan Kawasan Penghantaran Barangan dan *Loading Area*** | |
| Kawasan penghantaran barangan dan *loading* area hendaklah dikawal dan perlu dipisahkan dari akses terus ke kawasan larangan. | **Bahagian Khidmat Pengurusan** |
| **7.3: Keselamatan Pejabat, Bilik, Dan Kemudahan** | |
| **Objektif:**<br>Melindungi premis dan aset Jabatan/ Agensi daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan. | |
| Kawasan larangan ditakrifkan sebagai kawasan yang aksesnya dihadkan kepada pegawai-pegawai yang diberi kuasa sahaja. Ini dilaksanakan untuk melindungi aset Jabatan/ Agensi yang terdapat di dalam kawasan tersebut. Kawasan larangan di Jabatan/ agensi adalah seperti Bilik Ketua Jabatan/ Agensi, Bilik Fail, Bilik Kebal, Bilik Senjata, Pusat Data, Bilik Simpanan Kunci, Pusat Pemulihan Bencana dan Pusat Kawalan CCTV serta mana-mana kawasan yang telah/ akan diisytiharkan sebagai kawasan larangan. Akses kepada bilik-bilik tersebut adalah terhad kepada pegawai-pegawai yang diberi kuasa sahaja. | **Semua** |
| **7.4: Pemantauan Keselamatan Fizikal** | |
| **Objektif:**<br>Melindungi premis dan aset Jabatan /Agensi daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan. | |
| Akses tanpa kebenaran ke kawasan fizikal terhad seperti bilik *server* dan bilik peralatan IT boleh mengakibatkan kehilangan | **Semua** |

| | |
|---|---|
| kerahsiaan, ketersediaan, integriti dan keselamatan aset maklumat.<br><br>Berikut adalah kawalan yang boleh dilaksanakan:<br><br>a) Pemasangan kamera CCTV di ruang dan perkarangan pejabat;<br><br>b) menyediakan Pengawal keselamatan di pos masuk utama;<br><br>c) menghadkan akses ke Pusat Data dan terhad kepada pegawai yang diberi kebenaran. Bagi kemasukan selain pegawai yang diberi kebenaran ke kawasan tersebut perlu direkodkan di dalam buku rekod keluar/masuk pusat data dan diiringi oleh pegawai ICT yang berkenaan;<br><br>d) pemantauan kad akses melalui sistem yang disediakan; dan<br><br>e) pendaftaran pelawat/pelanggan di pintu masuk utama. | |
| **7.5: Perlindungan Fizikal Dan Ancaman Persekitaran** | |
| **Objektif:**<br><br>Melindungi aset Jabatan/ agensi dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan. | |
| Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset Jabatan/ Agensi, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Bahagian Teknologi Maklumat Dan Komunikasi (BTMK) dan Jabatan Kerja Raya (JKR).<br><br>Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi:-:<br><br>a) Merancang dan menyediakan pelan keseluruhan susun atur ruang pejabat seperti bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya dengan teliti;<br><br>b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan | **Bahagian Khidmat Pengurusan** |

| | |
|---|---|
| keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;<br>c) peralatan perlindungan keselamatan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;<br>d) bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset Jabatan/ Agensi;<br>e) semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset Jabatan/ Agensi ;<br>f) pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer;<br>g) semua peralatan perlindungan hendaklah disemak dan diuji secara berkala. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu;<br>h) akses kepada saluran *riser* hendaklah sentiasa berkunci; dan<br>i) kawalan serangga perosak dijalankan secara berkala | |
| **7.6: Bekerja Di Kawasan Yang Selamat** | |
| **Objektif:**<br>Melindungi premis dan aset Jabatan/ Agensi daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan | |
| **7.6.1: Kawasan Larangan** | |
| Kawasan larangan mempunyai ciri-ciri keselamatan yang tinggi seperti berikut;<br>a. Pemantauan dibuat menggunakan kamera *CCTV* atau lain-lain peralatan yang sesuai;<br>b. peralatan keselamatan (*CCTV*, log akses) perlu diperiksa secara berjadual; | **Semua** |

| | |
|---|---|
| c. butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan;<br>d. pelawat/ pihak ketiga yang dibawa masuk mesti diiringi oleh pegawai yang bertanggungjawab sepanjang tempoh di lokasi berkaitan;<br>e. memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan;<br>f. menyediakan tempat atau bilik khas untuk pelawat;<br>g. peralatan ICT di dalam kawasan larangan hendaklah dijaga dan dikawal supaya sentiasa dalam keadaan selamat, baik dan boleh digunakan; dan<br>h. semua penggunaan peralatan yang melibatkan penghantaran, pengemaskinian dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan/ Agensi. | |
| **7.7: Dasar Meja Kosong Dan Skrin Kosong** | |
| **Objektif:**<br>Mengurangkan risiko capaian yang tidak dibenarkan ke atas maklumat semasa dan di luar waktu kerja biasa. | |
| Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja atau di paparan skrin apabila kakitangan tidak berada di tempatnya.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:-:<br>a. Menggunakan kemudahan password *screen saver* atau *logout* apabila meninggalkan komputer; | **Semua** |

| | |
|---|---|
| b. semua komputer tidak boleh ditinggalkan dalam keadaan *logged on* tanpa kehadiran pengguna; kecuali telah disetkan *auto lock* selepas 5 minit atau tempoh masa yang ditetapkan bagi menghalang pengguna lain menggunakan komputer berkenaan sewaktu ditinggalkan;<br>c. bahan-bahan sensitif/ dokumen terperingkat hendaklah disimpan dalam laci atau kabinet fail yang berkunci apabila meninggalkan meja kerja; dan<br>d. memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin *faksimile* dan mesin fotostat. | |

**7.8: Lokasi Dan Perlindungan Peralatan**

**Objektif:**

Melindungi peralatan Jabatan/ Agensi dari kehilangan dan perkara-perkara yang boleh membahayakan.

| | |
|---|---|
| Dalam memastikan peralatan dikawal dan dijaga dengan baik, perkara-perkara yang perlu dipatuhi adalah seperti berikut :-<br>a) Pengguna hendaklah bertanggungjawab menyemak dan memastikan semua perkakasan di bawah kawalannya berfungsi dengan sempurna dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;<br>b) pengguna hendaklah memastikan semua perkakasan disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan;<br>c) semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran dan tidak digunakan untuk tujuan peribadi; | **Semua** |

| | |
|---|---|
| d) pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan serta membuat instalasi sebarang perisian tambahan tanpa kebenaran Pemilik Aset ICT;<br><br>e) pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;<br><br>f) perisian *antivirus* di komputer peribadi sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;<br><br>g) penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;<br><br>h) sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Unit Teknologi Maklumat untuk di baik pulih;<br><br>i) peralatan-peralatan kritikal seperti *server* perlu disokong oleh *Uninterruptable Power Supply* (*UPS*);<br><br>j) semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan di dalam rak khas;<br><br>k) semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;<br><br>l) peralatan ICT yang hendak dibawa keluar dari premis Jabatan/ Agensi, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan; | |

| | |
|---|---|
| m) peralatan ICT yang hilang hendaklah dilaporkan kepada Pegawai Aset dengan segera;<br><br>n) pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;<br><br>o) pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset;<br><br>p) sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;<br><br>q) konfigurasi alamat *IP* tidak dibenarkan diubah daripada alamat *IP* yang asal;<br><br>r) pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Unit Teknologi Maklumat. Kata laluan bagi pentadbir (*administrator password*) adalah terhad untuk pengetahuan pentadbir sistem sahaja;<br><br>s) pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;<br><br>t) pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dimatikan apabila meninggalkan pejabat;<br><br>u) sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada Unit Teknologi Maklumat;dan | |

| | |
|---|---|
| v) memastikan soket dimatikan daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya. | |
| **7.9: Keselamatan Aset di Luar Premis** | |
| **Objektif:**<br>Mengelakkan kehilangan, kerosakan, kecurian atau gangguan kepada operasi organisasi. | |
| Langkah-langkah yang perlu dipatuhi bagi perkakasan yang dibawa keluar dari permis Jabatan/ Agensi adalah seperti di bawah:<br>a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan dengan menggunakan Borang KEW-PA 9;<br>b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan;<br>c. Peralatan perlu dilindungi dan dikawal sepanjang masa;<br>d. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian dan sebarang kehilangan peralatan adalah di bawah tanggungjawab individu yang membawa keluar peralatan tersebut;<br>e. Kehilangan sebarang peralatan yang dibawa keluar hendaklah dimaklumkan segera kepada Pegawai Aset ICT dan proses hapus kira perlu dilaksanakan mengikut tatacara yang dinyatakan di dalam Pekeliling Perbendaharaan (PP) ; dan<br>f. Permohonan akses VPN perlu direkodkan. | **Semua** |

| 7.10: Media Storan | |
|---|---|
| **Objektif:**<br>Memastikan agar pengubahsuaian, penyingkiran atau pemusnahan maklumat pada storan media dilaksanakan sewajarnya. | |
| Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti cakera padat, *thumb drive,* pengkomputeran awan dan media storan lain.<br>Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat:-:<br>a) Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;<br>b) Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja;<br>c) Bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu melalui proses sanitasi data;<br>d) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu dan dihapuskan dengan teratur dan selamat;<br>e) Pengguna bertanggungjawab terhadap keselamatan maklumat dalam storan mudah alih seperti *thumbdrive* atau *external harddisk*; | **Semua pengguna**<br>**Pegawai Aset ICT** |

| | |
|---|---|
| f) Perkakasan sandaran (*backup*) hendaklah diletakkan di tempat yang terkawal. Storan dan peralatan sandaran (*backup*) hendaklah disimpan di lokasi yang berasingan dan tidak terbuka kepada umum atau mengikut keperluan; dan<br>g) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat. | |
| **7.11: Utiliti Sokongan** | |
| **Objektif:**<br>Memastikan agar peralatan dan perkakasan yang memproses maklumat dapat dilindungi dari terputusnya bekalan kuasa. | |
| Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.<br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:-:<br>a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT;<br>b) Peralatan sokongan seperti *Uninterruptable Power Supply* (*UPS*) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik Pusat Data supaya mendapat bekalan kuasa berterusan; dan<br>c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual. | **Semua Pengguna, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan/ Agensi** |

| 7.12: Keselamatan Kabel | |
|---|---|
| **Objektif:**<br>Memastikan segala jenis kabel yang digunakan dalam operasi harian keselamatan maklumat telah dilindungi dari ancaman. | |
| Kabel elektrik komputer dan kabel telekomunikasi komputer hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah:-:<br>a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan dan mendapat pengesahan daripada pihak pengilang/pengeluar;<br>b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;<br>c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan<br>d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel terutamanya daripada kerosakan dan pintasan maklumat. | **Bahagian Khidmat Pengurusan/**<br><br>**Unit Teknologi Maklumat** |
| **7.13: Penyelenggaraan Perkakasan** | |
| **Objektif:**<br>Perkakasan ICT hendaklah diselenggara mengikut jadual bagi memastikan ianya *Confidentiality*, *Integrity* dan *Accessebility* (CIA) dan di dalam keadaan selamat. | |
| Perkakasan hendaklah diselenggara agar tidak bermasalah bagi memastikan kebolehsediaan, kerahsiaan dan integriti.<br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:-: | **Unit Teknologi Maklumat** |

| | |
|---|---|
| a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan;<br>b. perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;<br>c. bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;<br>d. semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan;<br>e. memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan<br>f. semua penyelenggaraan mestilah mendapat kebenaran daripada pegawai. | |
| **7.14: Pelupusan Selamat Atau Penggunaan Semula Peralatan** | |
| **Objektif:**<br>Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh Jabatan/ Agensi dan ditempatkan di Jabatan/ Agensi . | |
| Peralatan ICT yang hendak dilupuskan atau diguna semula terutama yang mengandungi maklumat terperingkat atau perisian yang dilesenkan, perlu diuruskan dengan teratur dan selamat melalui prosedur pelupusan semasa atau guna semula peralatan yang telah ditetapkan. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan Jabatan/ Agensi . | **Semua** |

| | |
|---|---|
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:-:<br>a. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh diguna semula atau dilupuskan;<br>b. Semua kandungan peralatan ICT khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum diguna semula atau pelupusan dilakukan;<br>c. Peralatan ICT yang akan dilupus atau dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;<br>d. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan (salinan maklumat);<br>e. Peralatan ICT hendaklah di *format* atau diubah kepada keadaan asal *(set to factory setting)* sebelum diguna semula atau dilupuskan.<br>f. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;<br>g. Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemaskini rekod pelupusan pada kad harta modal sedia ada; dan<br>h. Pelupusan oleh pihak ketiga hendaklah dilakukan mengikut tatacara pelupusan dan menyediakan bukti penyaksian pelupusan. | |

| | |
|---|---|
| Semua pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:-:<br>a) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk menjadi milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman *CPU* seperti *RAM, harddisk, motherboard, modem* dan sebagainya;<br>b) Menyimpan dan memindahkan perkakasan luaran komputer seperti *mouse, keyboard, speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di Jabatan/ Agensi ;<br>c) Memindah keluar dari Jabatan/ Agensi mana-mana peralatan ICT yang hendak dilupuskan;<br>d) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab Jabatan/ Agensi; dan<br>e) Semua kakitangan bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti *thumb drive* atau *external hard disk* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan. | |

| PERKARA | PERANAN |
|---|---|
| **BIDANG 8 – KAWALAN TEKNOLOGI** | |
| **8.1: Peranti Akhir Pengguna** | |
| **Objektif:** | |
| Melindungi maklumat yang disimpan, diproses dan dicapai daripada sebarang bentuk pencerobohan, ancaman dan kerosakan melalui peranti pengguna akhir. | |
| Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut:<br>a. Peralatan mudah alih yang dibekalkan oleh Jabatan/ Agensi seperti (tablet, komputer riba, telefon pintar dan seumpamanya) yang dikhaskan untuk pegawai yang berkelayakan dibenarkan dibawa keluar bagi melaksanakan tugas-tugas rasmi;<br>b. Peralatan mudah alih gunasama perlu direkod dan mendapat kelulusan pegawai yang bertanggungjawab apabila hendak dibawa keluar dari pejabat;<br>c. Semua peralatan mudah alih hendaklah dilindungi dan dikawal dengan selamat;<br>d. Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan;<br>e. Tamatkan sesi aktif apabila selesai tugas;<br>f. Mewujudkan password yang unik bagi peralatan baru;<br>g. *Reset factory* apabila bertukar pemilik; dan<br>h. *Log-off* komputer apabila sesi bertugas selesai; | **Semua** |

| | |
|---|---|
| **8.2: Hak Capaian Istimewa** | |
| **Objektif:**<br>Memastikan hanya pengguna yang dibenarkan, komponen perisian dan perkhidmatan disediakan diberi hak capaian istimewa. | |
| **8.2.1: Pengurusan Hak Capaian Istimewa** | |
| Penggunaan *Priviledged Access Rights* perlu dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas. | **Semua** |
| **8.3: Sekatan Capaian Maklumat** | |
| **Objektif ;**<br>Memastikan hanya capaian yang dibenarkan dan menghalang capaian yang tidak dibenarkan ke atas maklumat dan lain-lain aset berkaitan (rangkaian atau sistem). | |
| Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi:<br>a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang diberikan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;<br>b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log);<br>c) Menghadkan capaian sistem dan aplikasi kepada maksima lima (5) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;<br>d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan seperti firewall, WAF, Antivirus dan IPS bagi mengelakkan aktiviti atau capaian yang tidak sah;<br>e) Capaian aset ICT sistem maklumat dan aplikasi melalui jarak jauh adalah dibenarkan dengan kelulusan | **Semua** |

| | |
|---|---|
| ICTSO/Ketua Unit Keselamatan dan Rangkaian. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja berdasarkan Arahan Keselamatan (Semakan dan Pindaan 2017);<br>f) Semua sistem yang mendatangkan risiko yang tinggi kepada operasi Jabatan/ Agensi perlu di asingkan daripada capaian terus melalui internet; dan<br>g) Pengasingan kepada sistem-sistem ini perlu dilaksana dengan menggunakan VLAN/VPN dan zon rangkaian (intranet, DMZ, Internet). | |
| **8.4: Capaian Kepada Kod Sumber** | |
| **Objektif:**<br>Untuk mengelakkan fungsi yang tidak sah, elakkan perubahan yang tidak disengajakan atau berniat jahat dan untuk mengekalkan kerahsiaan harta intelek yang berharga. | |
| Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:-:<br>a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;<br>b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan Jabatan/ Agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal;<br>c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja bagi mengelakkan | **Unit Teknologi Maklumat** |

| | |
|---|---|
| kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian;<br>d) Capaian kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan<br>e) Menghalang sebarang peluang untuk membocorkan maklumat; dan<br>f) Log audit perlu dikekalkan kepada semua akses kepada kod sumber. | |
| **8.4.1: Pembangunan Aplikasi Secara *Outsource*** | |
| Pembangunan aplikasi secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (*source code*) bagi semua aplikasi adalah menjadi hak milik Jabatan/ Agensi. | **Unit Teknologi Maklumat** |
| **8.5: Pengesahan Keselamatan Lepas Rehat (*Secure Authentication*)** | |
| **Objektif:**<br>Memastikan pengguna yang ditentusahkan sahaja yang dibenarkan mencapai aset ICT serta aplikasi sistem. | |
| Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, Pentadbir Sistem perlu mengambil langkah-langkah berikut:<br>a) Akaun yang diperuntukkan oleh Jabatan/ Agensi sahaja boleh digunakan;<br>b) Mewujudkan teknik pengesahan mengikut kesesuaian sistem bagi semua sistem kritikal;<br>c) Akaun pengguna (*user id*) hendaklah unik;<br>d) Pemilik akaun pengguna bukanlah hak mutlak pengguna dan ia tertakluk kepada peraturan Jabatan/ Agensi. Akaun boleh ditarik balik jika pengguna melanggar peraturan;<br>e) Tidak semua pengguna boleh capai semua peringkat maklumat. Terdapat peringkat dalam capaian maklumat dengan dikawal menggunakan akaun. Sebarang | **Pentadbir Sistem Aplikasi** |

| | |
|---|---|
| perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu melalui Borang C: Borang Permohonan/ Perubahan Sistem/ Operasi ICT;<br>f) Pengguna yang tidak aktif mengikut tempoh masa yang ditetapkan hendaklah disemak semula;<br>g) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan<br>h) Akaun pengguna boleh dibekukan dan ditamatkan atas sebab-sebab berikut:<br>i. Bertukar bidang tugas kerja;<br>ii. Bertukar ke agensi lain;<br>iii. Bersara;<br>iv. Digantung perkhidmatan ;<br>v. Ditamatkan perkhidmatan; atau<br>vi. Akaun telah dikompromi. | |
| **8.6: Pengurusan Kapasiti** | |
| **Objektif;**<br>Memastikan kemudahan kapasiti pemprosesan maklumat, sumber manusia, pejabat dan kemudahan lain yang diperlukan bagi minimumkan risiko yang menyebabkan gangguan atau kegagalan sistem. | |
| a. Penggunaan aplikasi atau sistem hendaklah dipantau dari semasa ke semasa. Kajian perancangan perlu dilakukan setiap tahun bagi memastikan tahap perkhidmatan yang disasarkan tercapai. Perkara-perkara yang perlu dilakukan adalah:<br>i. Menentukan keupayaan perkakasan seperti CPU dan *Random Access Memory* (RAM); dan<br>ii. Memastikan kapasiti storan mencukupi melalui penggunaan sistem pemantauan perkakasan atau hasil penyelenggaraan berkala peralatan di Jabatan/ Agensi. | **Unit Teknologi Maklumat / Sumber Manusia/ Khidmat Pengurusan** |

| | |
|---|---|
| b. bahagian ICT Jabatan/ Agensi hendaklah memantau semua sumber secara berkala atau sekurang-kurangnya sekali setahun bagi menentukan keupayaan perkakasan sedia ada melalui penggunaan suatu sistem pemantauan perkakasan dan rangkaian serta hasil penyelenggaraan berkala peralatan ICT di Jabatan/ Agensi;<br>c. peningkatan dan penambahbaikan perkakasan hendaklah dirancang dan diperolehi untuk mencapai tahap perkhidmatan yang disasarkan;<br>d. pengumpulan data hendaklah mengambil kira semua penggunaan sistem yang tinggi dan sederhana serta mengkaji tahap peningkatan yang sesuai dengan keperluan dan kos;<br>e. bajet dan jangka masa hendaklah diambilkira semasa membuat perancangan naik taraf atau gantian sistem; dan<br>f. kos naik taraf hendaklah dibandingkan dengan kos gantian serta tempoh sokongan (*support*) perkakasan oleh pembekal sebelum sesuatu keputusan dibuat. | |
| **8.7: Perlindungan Terhadap Perisian *Malware*** | |
| **Objektif:**<br>Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya. | |
| Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan malware hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. | **Semua** |

| | |
|---|---|
| Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya adalah seperti berikut :<br>a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti Antivirus, Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS), Content filtering dan Web Application Firewall (WAF) serta mengikut prosedur penggunaan yang betul dan selamat;<br>b) memasang dan menggunakan hanya perisian yang asli, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;<br>c) memastikan perisian antivirus mempunyai pengurusan berpusat bagi memudahkan penetapan polisi dan penyediaan laporan jika berlaku virus *outbreak* dalam rangkaian;<br>d) mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya serta dilaksanakan secara berkala;<br>e) mengemas kini antivirus dengan *signature/pattern* terkini;<br>f) 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 ralat; dan<br>g) memberi amaran mengenai ancaman keselamatan siber seperti serangan virus, malware dan *hacker*. | |

## 8.8: Pengurusan Kelemahan Teknikal

**Objektif:**

Pengurusan kelemahan teknikal dalam keselamatan maklumat merujuk kepada proses mengenal pasti, menilai, dan mengurangkan kelemahan teknikal dalam sistem komputer, rangkaian dan aplikasi. Kelemahan Teknikal ialah kelemahan atau kecacatan dalam reka bentuk, pelaksanaan atau konfigurasi sistem yang boleh

| | |
|---|---|
| dieksploitasi oleh penyerang untuk mendapatkan akses tanpa kebenaran atau menyebabkan kemudaratan. | |
| Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem aplikasi dan operasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a. Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi;<br>b. menganalisis tahap risiko kerentanan; dan<br>c. mengambil tindakan pengolahan dan kawalan risiko. | **Unit Teknologi Maklumat** |
| **8.9: Pengurusan Konfigurasi** | |
| **Objektif:**<br>Memastikan perkakasan, perisian, sistem aplikasi dan rangkaian berfungsi berdasarkan kawalan tetapan yang sepatutnya dan melindungi peranti daripada sebarang perubahan yang tidak dibenarkan atau pindaan yang tidak betul. | |
| Dalam melaksanakan proses pengurusan konfigurasi untuk meminimumkan risiko keselamatan maklumat:<br>a) Memastikan bilangan pengguna yang mempunyai keistimewaan pentadbir (*administrator privilege*) pada tahap minimum;<br>b) melumpuhkan (*disable*) sebarang identiti yang tidak digunakan atau tidak diperlukan;<br>c) memantau dengan teliti capaian kepada program penyelenggaraan, aplikasi utiliti dan tetapan dalaman;<br>d) memastikan jam disegerakkan (*synchronised*) bagi tujuan jejak (*log*) konfigurasi dengan betul dan membantu dalam sebarang siasatan di masa hadapan; | **Unit Teknologi Maklumat** |

| | |
|---|---|
| e) menukar sebarang kata laluan atau tetapan keselamatan asal (*default*) yang dibekalkan dengan mana-mana peranti, perkhidmatan atau aplikasi;<br>f) melaksanakan log keluar secara automatik untuk mana-mana peranti, sistem atau aplikasi yang telah dibiarkan tidak aktif (*dormant*) dalam suatu tempoh masa tertentu;<br>g) memastikan semua keperluan pelesenan telah dipenuhi;<br>h) menguji setiap konfigurasi yang diperbaharui di dalam persekitaran penerimaan sebelum digunapakai dalam persekitaran sebenar apabila menaiktaraf aplikasi;<br>i) menjaga kerahsiaan konfigurasi;<br>j) mengguna tidak dibenarkan membuat sebarang pertukaran kepada konfigurasi yang telah ditetapkan;<br>k) pengguna tidak boleh mengubah konfigurasi alamat *IP* daripada alamat *IP* yang asal;<br>l) apabila bencana berlaku, sebelum konfigurasi baharu dibuat, sandaran (*backup*) hendaklah dibuat terlebih dahulu; dan<br>m) penyelenggaraan ke atas konfigurasi dilakukan dari masa ke semasa. | |
| **8.10: Pemadaman Maklumat** | |
| **Objektif:**<br>Pemadaman maklumat dalam keselamatan maklumat merujuk kepada proses mengalih keluar atau memusnahkan data dengan selamat daripada sistem komputer atau peranti storan. Ini termasuk pemadaman fail, *folder* dan keseluruhan *partition* atau cakera keras. Matlamatnya adalah untuk memastikan bahawa maklumat sensitif atau sulit tidak boleh dipulihkan oleh individu yang tidak dibenarkan dan untuk mengelakkan pelanggaran data. | |
| Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut; | **Semua** |

| | |
|---|---|
| a) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat;<br>b) penghapusan maklumat atau kandungan media mestilah dihapuskan dengan teratur dan selamat; dan<br>c) maklumat yang disimpan di dalam sistem informasi, peralatan dan mana-mana storan media perlu dihapuskan apabila tidak diperlukan menggunakan kaedah pemusnahan secara fizikal.<br><br>Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan Jabatan/ Agensi .<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br>a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan dilakukan;<br>b) sekiranya maklumat perlu disimpan, maka pengguna olehlah membuat penduaan;<br>c) peralatan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;<br>d) pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;<br>e) peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;<br>f) pegawai Aset bertanggungjawab merekodkan butir–butir pelupusan;<br>g) pelupusan peralatan ICT hendaklah dilakukan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan | |

h) peralatan ICT hendaklah di*format* atau diubah kepada keadaan asal *(set to factory setting)* sekiranya bersesuaian sebelum dilupuskan.

Semua kakitangan adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:

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

b) menyimpan dan memindahkan perkakasan luaran komputer seperti *AVR, speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di Jabatan/ Agensi;

c) memindah keluar dari Jabatan/ Agensi mana-mana peralatan ICT yang hendak dilupuskan tanpa kebenaran;

d) melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab Jabatan/ Agensi;

e) semua kakitangan bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan tambahan sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan; dan

f) pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana *Arahan Keselamatan* dan *Tatacara Jabatan Arkib Negara*.

## 8.11: Penyamaran Data

**Objektif**:

Bagi membataskan keterdedahan data sensitif (sebarang data yang boleh dianggap sebagai maklumat pengenalan peribadi (*Personal Identification Information* atau PII) dan mematuhi garis panduan, peraturan dan keperluan kontrak.

| | |
|---|---|
| *Data Masking* yang digunakan perlu mematuhi dasar organisasi mengenai kawalan akses dan dasar yang berkaitan, dan keperluan perkhidmatan, dengan mengambil kira perundangan yang berkenaan. Data sensitif hendaklah dilindungi menggunakan teknik *data masking* untuk mengelakkan pendedahan maklumat peribadi atau kritikal kepada pihak yang tidak berkenaan. | **Pentadbir Sistem** |
| **8.12: Pencegahan Kebocoran Data** | |
| **Objektif**:<br>Mengesan dan menghalang pendedahan dan pengekstrakan maklumat yang tidak dibenarkan oleh individu atau sistem. | |
| Langkah pencegahan kebocoran data hendaklah digunakan pada sistem, rangkaian dan sebarang peranti lain yang memproses, menyimpan atau menghantar maklumat sensitif. Langkah-langkah perlindungan kebocoran data juga boleh dilaksanakan untuk mengesan dan menghalang penghantaran data yang tidak dibenarkan. Semua aktiviti ini perlu mematuhi undang-undang, peraturan, dan piawaian yang relevan. | **Semua** |
| **8.13: Sandaran Maklumat** | |
| **Objektif:**<br>Membolehkan pemulihan daripada kehilangan data atau sistem. | |
| a) Semua media *backup* hendaklah digunakan mengikut panduan kegunaan dan bilangan kegunaan semula (maximum number of times *reusable or recycle*) dan tempoh kegunaan (*shelf life*) dari pembekal;<br>b) *Media backup* diuji dari semasa ke semasa untuk memastikan ia berfungsi dengan baik;<br>c) Rekod bagi jejak dan kitaran setiap media hendaklah disimpan; | **Semua** |

| | |
|---|---|
| d) *Media backup* perlu disimpan di bangunan berasingan yang sesuai dan selamat. Pastikan media dapat digunakan semasa pemulihan aplikasi atau sistem;<br>e) *Backup* perlu dilakukan apabila:<br>i. aplikasi atau sistem berubah atau naik taraf;<br>ii. Pangkalan data atau fail berubah;<br>f) Menyediakan jadual *backup* yang bersesuaian dengan kegunaan aplikasi;<br>g) Kekerapan aktiviti *backup* bergantung kepada pentingnya aplikasi atau sistem. Untuk setiap sistem *backup* penuh data (*full* data *backup*) perlu dilakukan sebulan sekali manakala *backup* data tambahan atau perubahan (*incremental or differential backup*) perlu dilakukan setiap hari;<br>h) Pastikan bahawa fail penting tidak disimpan dalam komputer peribadi atau komputer riba; dan<br>i) Pengguna hendaklah melakukan *backup* sendiri bagi fail-fail penting dan menyimpannya di tempat yang selamat. | |
| **8.14: Kemudahan Pemprosesan Maklumat Yang Bertindih** | |
| **Objektif:**<br>Memastikan operasi berterusan pada kemudahan pemprosesan maklumat. | |
| Pelan Pemulihan Bencana perlu diuruskan secara berikut:<br>a) Pelan Pemulihan Bencana perlu di simpan di lokasi Pusat Data Utama;<br>b) Fasiliti DRC perlu diwujudkan bagi memenuhi keperluan semasa; dan<br>c) Fasiliti DRC perlu diuji dari semasa ke semasa. | **Unit Teknologi Maklumat** |

| 8.15: Log | |
|---|---|
| **Objektif:**<br>Tujuan log adalah untuk merekod peristiwa, menghasilkan bukti, memastikan integriti maklumat log dan , menghalang akses yang tidak dibenarkan, mengenal pasti ancaman keselamatan maklumat yang boleh menyebabkan insiden keselamatan maklumat, sertadan menyokong penyiasatannya. | |
| 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, aktiviti- aktiviti 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 berikut :<br><br>i. fail log sistem pengoperasian;<br><br>ii. fail log servis (web, e-mel);<br><br>iii.fail log aplikasi (jejak audit); dan<br><br>iv.fail log rangkaian (*switch, firewall*, IPS)<br><br>Pentadbir Sistem Aplikasi/Perkhidmatan Digital hendaklah melaksanakan perkara-perkara berikut :<br><br>a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;<br>b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan | **Unit Teknologi Maklumat** |

| | |
|---|---|
| c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, pentadbir sistem hendaklah melaporkan kepada CSIRT Melaka. | |
| **8.16: Aktiviti Pemantauan** | |
| **Objektif:**<br>Aktiviti pemantauan dalam keselamatan maklumat merujuk kepada proses berterusan memantau dan menganalisis sistem dan aktiviti rangkaian untuk mengenal pasti dan bertindak balas terhadap potensi ancaman dan kelemahan keselamatan. | |
| Pentadbir Sistem mestilah bertanggungjawab mengesan, merekod dan menganalisis perkara-perkara berikut :<br>a) Sebarang percubaan pencerobohan kepada sistem ICT Jabatan/ Agensi ;<br>b) serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), spam, pemalsuan (*forgery phising*), pencerobohan (*instrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*);<br>c) pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;<br>d) aktiviti melayari, menyimpan atau mengedar bahan-bahan pornografi, berunsur fitnah dan propaganda anti kerajaan;<br>e) aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;<br>f) aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar *(bandwidth*) rangkaian;<br>g) aktiviti penyalahgunaan akaun e-mel; dan<br>h) aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran. | **Unit Teknologi Maklumat** |

| 8.17: Penyegerakkan Jam | |
|---|---|
| **Objektif:**<br>Penyegerakkan jam dalam keselamatan maklumat merujuk kepada proses memastikan bahawa jam pada sistem yang berbeza dan peranti yang berada di dalam rangkaian adalah tepat dan selari antara satu sama lain. | |
| Jam (masa) sistem harus disegerakkkan dengan servis NTP yang boleh dipercayai bagi memastikan log sistem tepat. | **Unit Teknologi Maklumat** |
| **8.18: Keistimewaan Penggunaan Program Utiliti** | |
| **Objektif:**<br>Memastikan penggunaan program utiliti tidak membahayakan sistem dan kawalan aplikasi untuk keselamatan maklumat. | |
| Penggunaan program utiliti dikawal ketat dan dihadkan serta perlu mematuhi perkara berikut:<br>a) Hanya program atau perisian khas utiliti yang selamat sahaja digunakan; dan<br>b) Penggunaan program utiliti perlulah dikawal dan dihadkan kepada pegawai yang dibenarkan saja. | **Unit Teknologi Maklumat** |
| **8.19: Pemasangan Perisian Pada Sistem Operasi** | |
| **Objektif:**<br>Menjamin integriti sistem operasi dan mencegah penyalahgunaan kelemahan teknikal. | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut :-<br>a) Pengguna dilarang sama sekali membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; | **Semua** |

| | |
|---|---|
| b) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;<br><br>c) Pengguna mesti memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;<br><br>d) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;<br><br>e) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem Aplikasi atau Juruteknik untuk di baik pulih;<br><br>f) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (*UPS*);<br><br>g) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;<br><br>h) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;<br><br>i) Peralatan ICT yang hendak dibawa keluar dari premis Jabatan/ Agensi, perlulah mendapat pengesahan kelulusan Pegawai Aset ICT dan direkodkan bagi tujuan pemantauan;<br><br>j) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset ICT dengan segera;<br><br>k) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; | |

| | |
|---|---|
| l) pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset ICT;<br><br>m) sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;<br><br>n) konfigurasi alamat *IP* tidak dibenarkan diubah daripada alamat *IP* yang asal;<br><br>o) pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Sistem Aplikasi/ Juruteknik. Kata laluan bagi pentadbir (*administrator password*) adalah terhad untuk pengetahuan pentadbir sistem sahaja. Selain itu, kata laluan ini juga perlu dicipta berdasarkan saranan polisi umum bagi kata laluan agar ianya kukuh dan tidak mudah diketahui oleh pihak lain. Kata laluan ini juga hendaklah diubah secara berkala bagi mengelakkan kebocoran yang tidak diingini;<br><br>p) pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;<br><br>q) pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dimatikan apabila meninggalkan pejabat;<br><br>r) sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO atau Pegawai Aset ICT;<br><br>s) memastikan soket dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum | |

| | |
|---|---|
| meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya;<br><br>t) memastikan setiap pemasangan aplikasi ataupun perisian hendaklah direkodkan, dan aplikasi ataupun perisian harus diuji dan dikemaskini sebelum dipasang dalam sistem *live* (*production*);<br><br>u) satu strategi *rollback* harus diadakan sebelum perubahan dilaksanakan;<br><br>v) versi perisian perlu disimpan sebagai pelan konfigurasi; dan<br><br>w) versi lama perisian perlu diarkibkan bersama dengan maklumat dan parameter, prosedur, maklumat konfigurasi terperinci dan perisian yang menyokongnya selama mana data boleh disimpan didalam arkib (*archive*). | |
| **8.20: Kawalan Keselamatan Rangkaian** | |
| **Objektif:**<br><br>Memastikan maklumat dalam rangkaian dilindungi. | |
| **8.20.1: Kawalan Infrastruktur Rangkaian** | |
| Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran. Kawalan capaian pekhidmatan rangkaian hendaklah dijamin selamat dengan:<br>a. Memastikan hanya pengguna yang dibenarkan sahaja boleh mendapat perkhidmatan rangkaian Melaka*Net;<br>b. menempatkan, mengasingkan atau memasang peralatan ICT yang bersesuaian untuk kawalan keselamatan antara rangkaian Melaka* Net, rangkaian agensi lain dan rangkaian awam; | **Unit Teknologi Maklumat** |

| | |
|---|---|
| c. mewujud, menguatkuasakan dan memantau mekanisme untuk pengesahan pengguna, ID pengguna, kata laluan atau peralatan ICT yang dihubungkan ke rangkaian; dan<br>d. memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT. | |
| **8.21: Keselamatan Perkhidmatan Rangkaian** | |
| **Objektif:**<br>Memastikan keselamatan dalam penggunaan perkhidmatan rangkaian. | |
| Pengurusan bagi semua perkhidmatan rangkaian merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian. Perkara-perkara yang perlu dilaksanakan adalah seperti berikut:-:<br>a) Pengurusan sistem rangkaian maklumat;<br>b) Pemantauan perkhidmatan rangkaian; dan<br>c) Penyelenggaraan firewall dan peralatan keselamatan rangkaian yang lain perlu dibuat dari masa ke semasa. | **Unit Teknologi Maklumat** |
| **8.22: Pengasingan Rangkaian** | |
| **Objektif:**<br>Memisahkan rangkaian dalam sempadan keselamatan dan mengawal trafik berdasarkan keperluan semasa. | |
| Pengasingan rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian Jabatan/ Agensi . | **Unit Teknologi Maklumat** |

| | |
|---|---|
| **8.23: Tapisan Laman Web** | |
| **Objektif:**<br>Menghapuskan risiko keselamatan yang mungkin timbul akibat capaian kepada laman web luaran dengan kandungan berniat jahat atau laman web yang tidak dibenarkan. | |
| Penggunaan *Web Content Filtering* atau kawalan capaian Internet yang bersesuaian untuk menyekat aktiviti/capaian laman web yang dilarang. | **Unit Teknologi Maklumat** |
| **8.24: Penggunaan Kriptografi** | |
| **Objektif:**<br>Memastikan penggunaan kriptografi adalah betul dan berkesan untuk melindungi kerahsiaan, ketulenan atau integriti maklumat mengikut keperluan. | |
| **8.24.1: Enkripsi** | |
| Proses enkripsi (*encryption*) perlu dilaksanakan bagi melindungi kerahsiaan maklumat kritikal atau sensitif berdasarkan keperluan, penilaian risiko dan selaras dengan peraturan Kerajaan Negeri Melaka.<br>Jabatan/ Agensi hendaklah mengguna pakai kawalan kriptografi seperti SSL, e-mel dan enkripsi kata laluan yang mematuhi undang-undang dan peraturan-peraturan Kerajaan Malaysia. | **Semua** |
| **8.24.2: Tandatangan Digital** | |
| Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya yang berurusan dengan transaksi maklumat kritikal atau sensitif atau maklumat rahsia rasmi secara elektronik.Maklumat rahsia rasmi yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan. | **Semua** |

| 8.25: Kitaran Hidup Pembangunan Yang Selamat | |
|---|---|
| **Objektif:**<br>Memastikan keselamatan maklumat direka dan dilaksanakan dalam kitar hayat pembangunan yang selamat bagi perisian dan sistem. | |
| Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:<br>a) Keselamatan persekitaran pembangunan;<br>b) Keselamatan pangkalan data;<br>c) Keperluan keselamatan dalam fasa reka bentuk;<br>d) Keperluan check point keselamatan dalam carta perbatuan projek;<br>e) Keperluan pengetahuan ke atas keselamatan aplikasi;<br>f) Keselamatan dalam kawalan versi; dan<br>g) Bagi pembangunan secara penyumberluaran (*outsource*), pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sesuatu perisian atau aplikasi. | **Unit Teknologi Maklumat** |

| 8.26: Keperluan Keselamatan Aplikasi |
|---|
| **Objektif:**<br>Keperluan keselamatan aplikasi dalam keselamatan maklumat merujuk kepada satu set garis panduan dan piawaian yang digunapakai oleh Jabatan/ Agensi untuk memastikan bahawa aplikasi perisian mereka selamat dan bebas daripada kelemahan. |

| | |
|---|---|
| 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:<br>a) Memastikan pembekal yang dipertanggungjawabkan mempunyai kelayakan dalam bidang berkaitan dan pembekal yang berdaftar dengan Kementerian Kewangan;<br>b) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna;<br>c) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan;<br>d) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan;<br>e) Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data; dan<br>f) Pelaksanaan aktiviti keselamatan ICT seperti *Penetration Testing* dan sebagainya boleh dilakukan terhadap sistem-sistem utama. | **Unit Teknologi Maklumat** |
| **8.27: Prinsip Senibina Sistem dan Kejuruteraan Yang Selamat** | |
| **Objektif:**<br>Memastikan sistem maklumat direka, dilaksanakan, dan beroperasi dengan selamat dalam kitar hayat pembangunan | |

| | |
|---|---|
| Keselamatan perlu diambil kira dalam semua peringkat Pembangunan sistem. Prinsip dan prosedur keselamatan ICT hendaklah sentiasa dikaji dari semasa ke semasa bagi memastikan keberkesanan keselamatan maklumat. | **Unit Teknologi Maklumat** |
| **8.28: Pengekodan Selamat** | |
| **Objektif:**<br>Pengekodan selamat merujuk kepada amalan menulis kod komputer yang selamat dan kurang terdedah kepada serangan. Ia melibatkan penggunaan teknik dan kaedah untuk menghalang kelemahan keselamatan daripada diperkenalkan ke dalam kod semasa proses pembangunan.<br>Ini termasuk amalan reka bentuk dan pengekodan yang meminimumkan risiko perisian biasa kelemahan seperti *Buffer Overflow, SQL Injection* dan *cross-site scripting*. Pengekodan selamat juga termasuk piawaian, garis panduan dan amalan terbaik. Selain itu, pengekodan selamat juga termasuk menguji dan menyemak kod untuk mengenal pasti dan membetulkan sebarang isu keselamatan sebelum penggunaan | |
| Organisasi harus memastikan prinsip pengekodan selamat dipatuhi untuk kedua-dua produk perisian yang diperoleh daripada pihak luar dan kepada komponen perisian sumber terbuka sama ada projek pengekodan baharu dan juga operasi penggunaan semula perisian meliputi aktiviti pembangunan perisian dalaman dan pemindahan produk atau perkhidmatan perisian organisasi kepada pihak ketiga.Prasyarat pengekodan selamat, organisasi harus mematuhi perkara berikut:<br>a) Menentukan jangkaan keselamatan yang disesuaikan dengan keperluan mereka dan mewujudkan prinsip yang diluluskan untuk pengekodan perisian yang selamat yang akan digunakan untuk kedua-dua pembangunan perisian secara dalaman dan komponen perisian sumber luar; | **Unit Teknologi Maklumat** |

| | |
|---|---|
| b) Mengesan dan mendokumentasikan amalan reka bentuk pengekodan yang paling lazim dan sejarah amalan pengekodan buruk serta kesilapan yang mengakibatkan kesan kepada keselamatan maklumat;<br><br>c) Menyediakan dan mengkonfigurasi alat pembangunan (*development tools*) perisian untuk memastikan keselamatan semua kod yang diwujudkan;<br><br>d) Mencapai pematuhan dengan panduan dan arahan yang disediakan oleh alat pembangunan (*development tools*) perisian;<br><br>e) Menyemak, menyelenggara dan menggunakan alat pembangunan (*development tools*) dengan selamat seperti *compilers*;<br><br>f) Panduan keselamatan pengekodan selamat:<br><br>i. Prinsip pengekodan perisian yang selamat harus disesuaikan dengan setiap bahasa pengaturcaraan dan teknik yang digunakan;<br><br>ii. Penggunaan teknik dan kaedah pengaturcaraan selamat seperti pembangunan dipacu ujian (*test-driven development*) dan pengaturcaraan pasangan (*pair programming*);<br><br>iii. Penggunaan kaedah pengaturcaraan berstruktur atau berorientasikan objek (*structured/object programming methods*);<br><br>iv. Dokumentasi kod yang betul dan penyingkiran kecacatan kod (*removal of code defects*);<br><br>v. Larangan ke atas penggunaan kaedah pengekodan perisian yang tidak selamat seperti sampel kod yang mempunyai kerentanan atau *hardcoded passwords*; | |

| | |
|---|---|
| vi. Ujian keselamatan dilakukan semasa dan selepas pembangunan mengikut **Kawalan 8.29.**<br><br>Sebelum meletakkan perisian itu persekitaran sebenar, organisasi harus mempertimbangkan perkara berikut:<br>a) Apakah permukaan serangan?<br>b) Adakah prinsip keistimewaan yang paling sedikit diikuti?<br>c) Melaksanakan analisis ke atas kesilapan pengaturcaraan yang paling lazim berlaku dan mendokumentasikan bahawa risiko ini telah dihapuskan.<br><br>Selepas kod digunakan dalam persekitaran sebenar:<br>a) Pengemaskinian harus digunakan dengan cara yang selamat;<br>b) Kerentanan keselamatan (*security vulnerabilities*) yang dilaporkan selaras dengan **Kawalan 8.8** harus ditangani;<br>c) Serangan yang disyaki terhadap sistem maklumat dan ralat hendaklah direkodkan dan rekod ini hendaklah disemak secara berkala supaya perubahan yang sesuai kepada kod boleh dibuat; dan<br>d) Capaian tanpa kebenaran kepada, penggunaan atau perubahan kepada kod sumber harus dihalang melalui mekanisme seperti alat pengurusan (*management tools*).<br><br>Apabila organisasi menggunakan alat (*tools*) luaran, perkara berikut harus diambil kira:<br>a) Perpustakaan luaran (*external libraries*) hendaklah dipantau dan dikemas kini pada selang masa yang tetap berdasarkan kitaran keluarannya;<br>b) Komponen perisian hendaklah disemak, dipilih dan dibenarkan dengan teliti terutamanya komponen kriptografi dan pengesahan; | |

| | |
|---|---|
| c) Pelesenan komponen luaran dan memastikan keselamatannya;<br>d) Perisian harus dijejaki dan diselenggara. Ia mesti dipastikan datang dari sumber yang boleh dipercayai;<br>e) Sumber pembangunan harus tersedia untuk jangka masa panjang.<br>Organisasi perlu memastikan kod berkaitan keselamatan digunakan apabila perlu dan tahan terhadap gangguan dengan mengambil kira perkara berikut:<br>a) Kod keselamatan berkesan apabila dijalankan pada pelayan yang tidak boleh diakses pengguna, diasingkan daripada proses lain dan dilindungi melalui kawalan capaian serta pengesahan yang kukuh;<br>b) Konfigurasi pelayan web yang sesuai perlu dilaksanakan bagi menghalang akses tanpa kebenaran dan penyemakan imbas direktori; dan<br>c) Kod aplikasi perlu direka bentuk dengan andaian wujud ancaman serangan dan ralat pengekodan, termasuk semakan keselamatan ke atas output sebelum digunakan dalam aplikasi kritikal. | |
| **8.29: Ujian Keselamatan Dalam Pembangunan Dan Penerimaan** | |
| **Objektif:**<br>Ujian keselamatan dalam pembangunan dan penerimaan ialah proses yang membantu mengenal pasti dan mengurangkan kelemahan keselamatan dalam aplikasi perisian sebelum ia digunakan. Ujian jenis ini biasanya dilakukan semasa fasa pembangunan dan penerimaan SDLC. | |
| Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut: | **Unit Teknologi Maklumat** |

| | |
|---|---|
| a) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat;<br>b) Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat; dan<br>c) Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan;<br>d) Melakukan imbasan kelemahan untuk mengenal pasti konfigurasi yang tidak selamat dan kelemahan sistem; dan<br>e) Skop dan tahap ujian keselamatan hendaklah ditentukan berdasarkan risiko dan kepentingan sistem. | |
| **8.30: Pembangunan Sumber Luar** | |
| **Objektif:**<br>Memastikan keperluan keselamatan maklumat yang ditetapkan dipatuhi oleh pembangun dari pihak ketiga (*outsourced*). | |
| Pembangunan aplikasi secara *outsource* perlu diselia dan dipantau oleh pegawai yang dipertanggungjawabkan. Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik Jabatan/ Agensi.<br>Perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Hak harta intelek, kod sumber dan data bagi sistem aplikasi yang dibangunkan adalah menjadi hak milik Jabatan/ Agensi;<br>b) Bagi semua perkhidmatan secara *outsource* dan terlibat dengan maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak perjanjian mesti menetapkan keperluan mandatori bahawa pembekal hendaklah membenarkan Jabatan/ agensi mendapatkan akses yang sewajarnya kepada kod sumber bagi tujuan penilaian dan pengurusan risiko keselamatan siber; | **Unit Teknologi Maklumat** |

| | |
|---|---|
| c) Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak ketiga mengikut amalan terbaik;<br>d) Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem;<br>e) Pemindahan teknologi (*Transfer Of Technology*) mesti dilaksanakan oleh kontraktor kepada pengguna;<br>f) Kontrak perjanjian perlu merangkumi pemilikan ke atas kod dan hak harta intelek;<br>g) Mengenakan keperluan kontrak yang sesuai untuk reka bentuk dan pengekodan selamat;<br>h) Menjalankan ujian penerimaan untuk memastikan kualiti dan ketepatan kerja yang dihantar;<br>i) Bukti bahawa keupayaan privasi dan keselamatan yang diperlukan secara minima telah dicapai. Ini boleh dicapai melalui laporan jaminan;<br>j) Merekod pengujian yang dilaksanakan untuk melindungi sistem atau perisian IT daripada kandungan berniat jahat (*malicious content*) dan kelemahan yang dikenal pasti;<br>k) Perjanjian escrow yang meliputi kod sumber perisian untuk menangani kemungkinan yang berlaku sekiranya pihak ketiga tidak lagi beroperasi;<br>l) Jabatan/ Agensi berhak untuk melaksanakan audit ke atas proses dan kawalan pembangunan; dan<br>m) Mematuhi dan mengambil kira semua undang-undang peraturan dan kehendak perundangan yang berkaitan. | |

| 8.31: Pengasingan Persekitaran Pembangunan, Pengujian Dan Pengeluaran | |
|---|---|
| **Objektif:**<br>Memastikan maklumat dan sistem organisasi dilindungi daripada akses, perubahan atau gangguan yang tidak dibenarkan dengan memisahkan persekitaran persekitaran aktiviti pengujian. | |
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br>a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;<br>b) Pengujian semula aplikasi perlu dipantau selepas perubahan sistem dilakukan oleh pihak ketiga;<br>c) Mengawal perubahan dan/atau pindaan ke atas aplikasi supaya terhad mengikut keperluan sahaja;<br>d) Akses kepada *source code* aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja; dan<br>e) Mencegah kebocoran maklumat;<br>f) Sistem pembangunan dan sistem persekitaran sebenar perlu diasingkan dan diurus dengan baik bagi mengelakkan kesilapan, gangguan operasi dan risiko keselamatan.;<br>g) Peraturan dan prosedur kebenaran yang sesuai hendaklah didokumenkan dan digunakan bagi peralihan aplikasi dari persekitaran pembangunan ke persekitaran sebenar;<br>h) Jabatan/ Agensi harus menyemak dan menguji perubahan yang dibuat pada aplikasi dan sistem dalam persekitaran pembangunan sebelum perubahan ini digunakan dalam persekitaran sebenar; | **Unit Teknologi Maklumat** |

| | |
|---|---|
| i) *Development tools* seperti *compilers* dan *editors* tidak boleh dicapai daripada persekitaran sebenar melainkan capaian ini benar-benar diperlukan;<br>j) Label dan identifikasi persekitaran digunakan untuk mengurangkan risiko kesilapan; dan<br>k) Maklumat sensitif hanya dibenarkan dalam pembangunan/ ujian jika keselamatannya setara dengan sistem sebenar. | |
| **8.32: Pengurusan Perubahan** | |
| **Objektif:**<br>Pengurusan perubahan dalam keselamatan maklumat merujuk kepada proses mengurus dan mengawal perubahan kepada sistem maklumat, aplikasi dan infrastruktur. Ini termasuk perubahan pada perkakasan, perisian dan konfigurasi rangkaian. | |
| **8.32.1: Kawalan Perubahan Perkakasan ICT** | |
| Perubahan yang melibatkan perkakasan rangkaian dan komunikasi, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah dikemukakan oleh pemilik sistem atau pentadbir rangkaian dan komunikasi dan mendapat kebenaran daripada pegawai yang diberi kuasa; dan<br>Sebarang perubahan komponen sistem ICT hendaklah mematuhi keperluan yang ditetapkan.<br>Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a. Pengubahsuaian yang melibatkan perkakasan rangkaian dan komunikasi, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;<br>b. aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen | **Semua** |

| | |
|---|---|
| ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;<br>c. semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan;<br>d. semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak; dan<br>e. Makluman kepada pengguna perlu dilakukan sekiranya perubahan mengakibatkan gangguan kepada perkhidmatan ICT. | |
| **8.32.2: Kawalan Perubahan Sistem ICT** | |
| Perubahan terhadap organisasi, proses, operasi, sistem dan fasiliti pemprosesan maklumat yang memberi kesan terhadap keselamatan maklumat perlu dikawal. Oleh itu, perkara yang perlu dipatuhi adalah seperti berikut:<br>a. Pengubahsuaian yang melibatkan peralatan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada Ketua Jabatan/ agensi Negeri atau pemilik aset ICT terlebih dahulu;<br>b. 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;<br>c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan;<br>d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat; dan | **Pentadbir Sistem Aplikasi** |

| | |
|---|---|
| e. Makluman kepada pengguna perlu dilakukan sekiranya perubahan mengakibatkan gangguan kepada perkhidmatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br>i. Perubahan dan pengubahsuaian ke atas sistem perisian aplikasi dan maklumat hendaklah dikawal, diuji, direkodkan dan disahkan melalui prosedur yang ditetapkan sebelum diguna pakai;<br>ii. Pengujian terhadap perubahan dan pengubahsuaian ke atas sistem perisian aplikasi dan maklumat hendaklah dilaksanakan dalam persekitaran yang berasingan samada daripada produksi atau pembangunan;<br>iii. 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;<br>iv. Mengawal perubahan dan/ atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;<br>v. Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan<br>vi. Menghalang sebarang peluang untuk membocorkan maklumat. | |
| **8.33: Maklumat Ujian** | |
| **Objektif:**<br>Memastikan data ujian direkod dan diuruskan dengan sewajarnya. | |

| | |
|---|---|
| Data ujian perlu dipilih, dilindungi dan dikawal dengan teliti, serta mengelakkan penggunaan data sebenar yang sensitif; jika digunakan, data sensitif mesti ditapis atau diubah suai.<br><br>Jabatan/ Agensi hendaklah mematuhi perkara berikut dalam melindungi maklumat sensitif, termasuk data peribadi, dalam pembangunan dan persekitaran pengujian:<br>a. Kawalan capaian yang digunakan dalam persekitaran sebenar juga harus dilaksanakan dalam persekitaran pembangunan;<br>b. Hanya individu yang dibenarkan sahaja boleh menyalin data dari persekitaran sebenar ke persekitaran pembangunan;<br>c. Merekodkan jejak audit bagi aktiviti yang berkaitan dengan penyalinan dan penggunaan maklumat dalam persekitaran pembangunan;<br>d. Melaksanakan kawalan yang sesuai seperti penyamaran data (*data masking*) atau penyingkiran data bagi tujuan perlindungan jika maklumat sensitif digunakan dalam persekitaran pembangunan; dan<br>e. Memastikan semua maklumat dalam persekitaran pembangunan dipadam secara selamat dan kekal selepas pengujian bagi mengelakkan risiko capaian tanpa kebenaran. | **Unit Teknologi Maklumat**<br><br>**Unit Keselamatan dan Rangkaian** |

**8.34: Perlindungan Sistem Maklumat Semasa Pengujian Audit**

**Objektif:**

Perlindungan sistem maklumat semasa ujian audit dalam keselamatan maklumat merujuk kepada langkah dan prosedur yang disediakan untuk melindungi sistem maklumat ketika ia diuji semasa audit.

| | |
|---|---|
| Keperluan dan aktiviti audit yang melibatkan pengujian sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses kelancaran sistem.Untuk melindungi sistem semasa pengujian audit, Jabatan/ Agensi boleh melaksanakan beberapa langkah:<br><br>a. Penggunaan akaun pengujian: gunakan akaun pengujian dan bukannya akaun sebenar untuk mengakses sistem semasa ujian. Ini boleh membantu untuk mengelakkan perubahan yang tidak disengajakan atau tidak dibenarkan pada sistem;<br><br>b. Penggunaan data pengujian: gunakan data pengujian dan bukannya data sebenar untuk melaksanakan pengujian. Ini boleh membantu untuk melindungi data sensitif atau data sulit daripada dikompromi;<br><br>c. Pengasingan persekitaran ujian: asingkan persekitaran ujian daripada persekitaran pengeluaran untuk mencegah gangguan atau kerosakan kepada persekitaran pengeluaran;<br><br>d. Sandaran data (*data backup*): lakukan sandaran sistem (*system backup*) sebelum pengujian - Perlu sekiranya sistem perlu dipulihkan apabila berlaku kejadian yang tidak dijangka;<br><br>e. Pemantauan: memantau sistem semasa pengujian untuk mengesan sebarang isu atau masalah yang mungkin berlaku; dan<br><br>f. Pelan pengujian: mempunyai pelan pengujian terperinci dan berkomunikasi dengan pihak yang berkaitan seperti pentadbir sistem dan pihak berkepentingan lain. | **Unit Teknologi Maklumat** |

| | |
|---|---|
| Keperluan khusus yang harus dipertimbangkan oleh Jabatan/ Agensi:<br><br>a. Pengurusan dan juruaudit harus bersetuju mengenai capaian kepada sistem dan aset maklumat;<br>b. Perjanjian mengenai skop pengujian audit teknikal yang akan dilaksanakan;<br>c. Jabatan/ Agensi hanya boleh menyediakan capaian baca sahaja (*read-only*) kepada maklumat dan perisian. Sekiranya tidak mungkin untuk menggunakan teknik baca sahaja, pentadbir yang mempunyai hak capaian yang diperlukan boleh mendapatkan capaian kepada sistem atau data bagi pihak juruaudit;<br>d. Jika permintaan capaian dibenarkan, Jabatan/ Agensi hendaklah terlebih dahulu mengesahkan bahawa peranti yang digunakan untuk mencapai sistem memenuhi keperluan keselamatan sebelum mereka menyediakan capaian;<br>e. Capaian hanya perlu disediakan untuk salinan fail terpencil (*isolated copies of files*) yang diekstrak daripada sistem. Salinan ini harus dipadamkan secara kekal setelah audit selesai melainkan terdapat keperluan untuk mengekalkan fail tersebut. Jika capaian baca sahaja boleh dilakukan, kawalan ini tidak terpakai;<br>f. Permintaan oleh juruaudit untuk melaksanakan pemprosesan khas seperti menggunakan alat audit (*audit tools*) perlu dipersetujui oleh pihak pengurusan;<br>g. Jika audit menyebabkan risiko yang menjejaskan ketersediaan sistem, audit hendaklah dijalankan di luar waktu operasi perkhidmatan untuk mengekalkan ketersediaan maklumat; dan<br>h. Permintaan capaian yang dibuat untuk audit hendaklah direkodkan untuk jejak audit. | |

**LAMPIRAN 1**

**DOKUMEN RUJUKAN**

Berikut adalah dokumen-dokumen yang dirujuk semasa penyediaan dokumen ini:

a) *MyMIS* – Garis Panduan Pengurusan Keselamatan ICT Sektor Awam Malaysia;
b) Akta Keselamatan (Semakan dan Pindaan 2017);
c) Akta Rahsia Rasmi 1972;
d) Akta Acara Kewangan 1957;
e) Akta Kawasan Larangan dan Tempat Larangan 1959;
f) Pekeliling Am Bil 3 Tahun 2000 – Rangka Polisi Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
g) Pekeliling Am Bil 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam;
h) Akta Jenayah Komputer 1997;
i) Akta Tandatangan Digital 1997;
j) Pekeliling Kemajuan Pentadbiran Awam Bil.1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan;
k) Arahan Perbendaharaan;
l) Portal Pekeliling Perbendaharaan (PPP)
m) Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) ;
n) Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; dan
o) Surat Pekeliling Am Bilangan 2 Tahun 2021: Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (*Cloud Computing*) Dalam Perkhidmatan Awam.

**LAMPIRAN 2**

**BORANG AKUAN PEMATUHAN**
**POLISI KESELAMATAN SIBER NEGERI MELAKA DAN**
**SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)**

Nama : ……
No. Kad Pengenalan : ……
Jawatan : ……
Jabatan / Bahagian : ……

Adalah dengan sesungguhnya dan sebenarnya saya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber Negeri Melaka dan ISMS; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan: …….

Tarikh : …….

**Pengesahan Ketua Pegawai Digital / Pegawai Keselamatan ICT**

……..
**(Nama)**
b.p Setiausaha Kerajaan Negeri Melaka

Tarikh: ……

## BORANG C: BORANG PERMOHONAN/ PERUBAHAN SISTEM/ OPERASI ICT

| No Siri | |
|---|---|

| MAKLUMAT PERMOHONAN | |
|---|---|
| NAMA : | NO.TELEFON : |
| JAB./BAH./UNIT : | E-MEL : |
| NAMA SISTEM/APLIKASI : | |
| PERUBAHAN/PERMOHONAN YANG DIPERLUKAN: | TANDATANGAN PEMOHON: |
| | TARIKH: |
| | PENGESAHAN PENYELIA: |
| | TARIKH: |
| **UNTUK KEGUNAAN PEJABAT SAHAJA** | |
| **KELULUSAN PEMILIK APLIKASI / SISTEM / DATA / KETUA UNIT** | |
| JENIS :<br>[ ] Permohonan Baru [ ] Kemaskini Capaian<br>[ ] Penambahbaikan<br>[ ] Pertambahan Modul/ *page* baru | COP & TANDATANGAN : |
| KEUTAMAAN : [ ] MINOR [ ] MAJOR [ ] KRITIKAL | TARIKH : |
| **TINDAKAN PEMBEKAL / PEMILIK APLIKASI / SISTEM / DATA** | |
| DESKRIPSI PERUBAHAN YANG DILAKUKAN : | COP & TANDATANGAN : |
| STATUS : [ ] SELESAI [ ] TANGGUH [ ] TOLAK | |
| VERSI LAMA (*jika ada*): / VERSI BARU (*jika ada*): | |
| | TARIKH : |
| **PENGESAHAN KETUA BAHAGIAN / UNIT** | |
| MAKLUMBALAS : | COP & TANDATANGAN : |
| | TARIKH : |
| **PENGESAHAN PEMOHON** | |
| MAKLUMBALAS/ CATATAN: | TANDATANGAN : |
| | TARIKH : |

| No Siri | |
|---|---|

BORANG J: PENAMATAN AKAUN APLIKASI DAN PEMULANGAN PERALATAN ICT

| MAKLUMAT PEMOHON | | | |
|---|---|---|---|
| Nama: | | | |
| No. K.P: | | | |
| Jawatan & Gred: | | | |
| Jabatan/Bahagian: | | | |
| No.Telefon: | | E-mel: | |
| Tarikh Tamat Perkhidmatan / Pertukaran: | | | |
| Sebab Penamatan: | ☐ Tamat Perkhidmatan | ☐ Pertukaran Dalaman | |
| | ☐ Pertukaran ke Jabatan Negeri | ☐ Pertukaran ke Jabatan Persekutuan/ Agensi | |

**PENGESAHAN KETUA JABATAN / PEMOHON**

Dengan ini adalah disahkan bahawa maklumat yang diberikan di atas adalah benar.

Nama :
Jawatan :
Tarikh : Tandatangan & Cop Rasmi

**UNTUK KEGUNAAN PEJABAT**

**MAKLUMAT AKAUN APLIKASI/ SISTEM**

| Senarai Aplikasi/ Sistem | Id | Dilaksanakan Oleh: | Tarikh: |
|---|---|---|---|
| Domain & E-mel Rasmi | | | |
| Lain-lain, sila nyatakan: | | | |
| **TINDAKAN** | ☐ Hapus | ☐ Kemaskini | ☐ Lain-lain _____ |

**MAKLUMAT PERALATAN ICT**

| Senarai Peralatan ICT | No. Rujukan: | Diterima Oleh: | Tarikh: |
|---|---|---|---|
| Komputer | | | |
| Printer | | | |
| Lain-lain, sila nyatakan: | | | |
| **TINDAKAN** | ☐ Hapus | ☐ Kemaskini | ☐ Lain-lain _____ |

Disemak/ Disahkan Oleh :

Tandatangan :
Tarikh :

| GLOSARI | |
|---|---|
| *Antivirus* | Perisian yang mengimbas *virus* pada media storan seperti disket, cakera padat, pita magnetik, optical disk, flash disk, CDROM, thumb drive untuk sebarang kemungkinan adanya *virus* |
| Aset ICT | Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia |
| *Backup* | Sandaran atau proses penduaan sesuatu dokumen atau maklumat. |
| *Bandwidth* | Lebar Jalur<br>Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan. |
| CDO | *Chief Digital Officer*<br>Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah Jabatan/ Agensi. |
| *Denial Of Service* | Halangan pemberian perkhidmatan |
| *Downloading* | Aktiviti muat-turun sesuatu perisian |
| *Encryption* | Enkripsi ialah satu proses penyulitan data oleh pengirim supaya 1tidak difahami oleh orang lain kecuali penerima yang sah |
| *Firewall* | Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya |
| *Forgery* | Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, |

| | |
|---|---|
| | pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*) |
| *Hard disk* | Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas |
| *Hub* | Hab (hub) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain |
| ICT | Information and Communication Technology (Teknologi Maklumat dan Komunikasi) |
| ICTSO | ICT Security Officer<br>Pegawai yang bertanggungjawab terhadap keselamatan sistem computer |
| Internet | Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain |
| *Internet Gateway* | Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan |
| *Intrusion Detection System* (IDS) | Sistem Pengesan Pencerobohan<br>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<br>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*.<br>Contohnya: *Network-based* IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan. |
| LAN | *Local Area Network*<br>Rangkaian Kawasan Setempat yang menghubungkan komputer |
| *Logout* | *Logout* komputer<br>Keluar daripada sesuatu sistem atau aplikasi komputer |
| *Malicious Code* | Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan *virus*, *trojan horse, worm, spyware* dan sebagainya |
| *MODEM* | MOdulator DEModulator<br>Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer. |
| *Outsource* | Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsifungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui |
| Perisian Aplikasi | Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi Jabatan/ Agensi atau jabatan |
| *Public-Key Infrastructure* (PKI) | Infrastruktur Kekunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang |

| | |
|---|---|
| | membolehkan organisasi Jabatan/ Agensi melindungi keselamatan berkomunikasi dan transaksi melalui internet |
| *Router* | Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, capaian internet. |
| *Screen Saver* | Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu |
| SDLC | *System Development Life Cycle*<br>- Kitaran Hayat Pembangunan Sistem |
| *Server* | Pelayan komputer |
| *Switches* | Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku. |
| *Threat* | Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu. |
| *Uninterruptible Power Supply* (UPS) | Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung |
| *Video Conference* | Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar. |
| *Video Streaming* | Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak. |
| *Virus* | Atur cara yang bertujuan merosakkan data atau sistem aplikasi |

| | |
|---|---|
| *Wireless* LAN | Jaringan komputer yang terhubung tanpa melalui kabel |