POLISI KESELAMATAN SIBER

MAJLIS BANDARAYA KUANTAN

VERSI 2.0

Bahagian Teknologi Maklumat
09-5121555/7511/7513
btm@mbk.gov.my

مجليس بندراي كوانتن
MAJLIS BANDARAYA
KUANTAN
CITY COUNCIL

Polisi Keselamatan Siber
(PKS)

Disediakan Oleh:	Disemak Oleh:	Diluluskan Oleh:
Nama:	Nama:	Nama:
Jawatan:	Jawatan:	Jawatan:
AZIRA BINTI AZAM Pen. Pegawai Teknologi Maklumat Kanan Bahagian Teknologi Maklumat Pejabat Datuk Bandar Majlis Bandaraya Kuantan	NURUL ASHIKIN BINTI AHMAD KHAIRUDIN Pengarah Bahagian Teknologi Maklumat Pejabat Datuk Bandar Majlis Bandaraya Kuantan	HAJI MOHD NIZAM BIN MAHAYUDDIN SMP., AAP. Setiausaha Majlis Bandaraya Kuantan

KANDUNGAN

ISI KANDUNGAN | **MUKA SURAT**

ISI KANDUNGAN | **MUKA SURAT**

SEJARAH POLISI KESELAMATAN SIBER MBK

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
27 Jun 2024	**1.0**	**Jawatankuasa Pemandu ICT (JKICT)**	**27 Jun 2024**
15 Disember 2025	**2.0**	**Mesyuarat Semakan Semula Pengurusan Sistem Pengurusan Keselamatan Maklumat (ISMS) Bil.2/2025**	**15 Disember 2025**

TUJUAN

Polisi Keselamatan Siber (PKS) Majlis Bandaraya Kuantan (MBK) ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh kakitangan Majlis Bandaraya Kuantan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Majlis Bandaraya Kuantan dalam melindungi maklumat di ruang siber.

LATAR BELAKANG

Polisi ini dibangunkan untuk menjamin kesinambungan urusan Majlis Bandaraya Kuantan dengan meminimumkan kesan insiden keselamatan siber. Polisi ini akan memudahkan perkongsian maklumat sesuai dengan keperluan operasi Majlis Bandaraya Kuantan bagi memastikan semua maklumat dilindungi.

OBJEKTIF

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

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

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

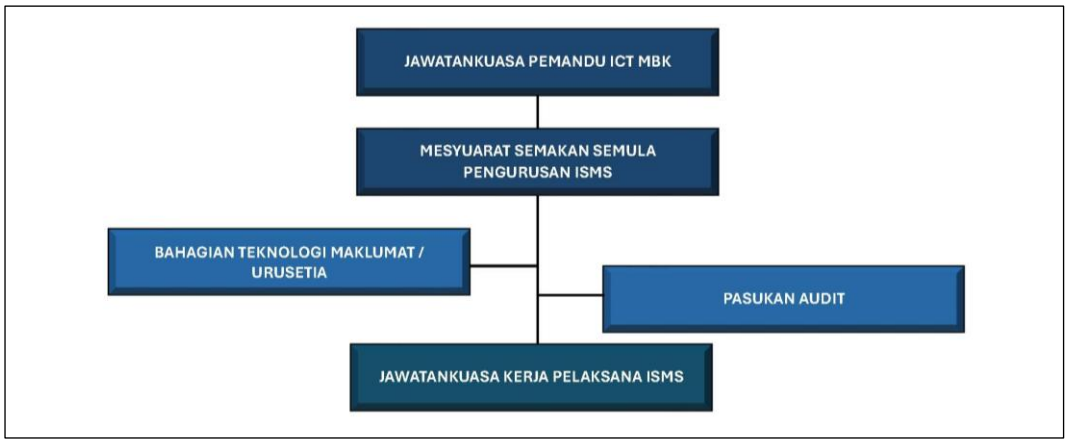
c. Memastikan kelancaran operasi Majlis Bandaraya Kuantan dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;

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

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

TADBIR URUS

Bagi memastikan keberkesanan dan kejayaan pelaksanaan PKS Majlis Bandaraya Kuantan, satu (1) struktur tadbir urus iaitu Jawatankuasa telah diwujudkan seperti berikut:



CARTA JAWATANKUASA ISMS MAJLIS BANDARAYA KUANTAN

PERANAN	TANGGUNGJAWAB
MESYUARAT JAWATANKUASA PEMANDU ICT	• Melaksanakan semakan pengurusan ke atas sistem pengurusan ISMS secara berkala bagi memastikan terus sesuai, mencukupi, dan berkesan; • Membuat penilaian ke atas peluang penambahbaikan dan keperluan perubahan kepada ISMS termasuk objektif keselamatan dan polisi keselamatan maklumat; dan • Meneliti laporan yang berkaitan dan membuat keputusan yang sesuai.
MESYUARAT SEMAKAN SEMULA PENGURUSAN ISMS	• Mesyuarat Semakan Semula Pengurusan adalah untuk menilai keberkesanan keseluruhan sistem pengurusan keselamatan maklumat dalam organisasi dan memastikan ia kekal relevan, mencukupi serta berfungsi dengan baik. • Mesyuarat ini digunakan untuk menyemak prestasi kawalan keselamatan, keputusan audit dalaman dan luaran, status tindakan pembetulan, perubahan risiko serta keperluan sumber. • Menilai isu-isu keselamatan terkini, maklum balas pihak berkepentingan, tahap pematuhan terhadap dasar dan objektif keselamatan serta peluang penambahbaikan. • Menetapkan arah tuju tindakan susulan.
BAHAGIAN TEKNOLOGI MAKLUMAT	• Menyelaras Hubungan Badan Pensijilan SIRIM • Merancang latihan berkaitan ISMS; • Urus setia kepada pelaksanaan Jawatankuasa ISMS; dan • Memantau tindakan susulan ke atas tindakan pembetulan dan peluang penambahbaikan ISMS serta menyelenggara rekod berkaitan.

PERANAN	TANGGUNGJAWAB
PASUKAN KERJA PELAKSANA ISMS	• Menyediakan analisis jurang, *Statement of Applicability* (SoA), penilaian risiko, pelan pemulihan risiko dan prosedur-prosedur; • Melaksanakan pelan pemulihan risiko*;* dan • Membangun dan mengukur keberkesanan kawalan ISMS.
PASUKAN AUDIT DALAMAN ISMS	• Melaksana Audit Dalaman ISMS berdasarkan keperluan standard. • Menyediakan Laporan Audit Dalaman ISMS; • Melaporkan penemuan Audit Dalaman ISMS ke Jawatankuasa Audit Dalaman ISMS dan Mesyuarat Semakan Semula Pengurusan (MSSP); dan • Menjalankan audit susulan bagi mengesahkan tindakan pembetulan yang dilaksanakan.

Peranan dan tanggungjawab Jawatankuasa ISMS

ASET ICT MAJLIS BANDARAYA KUANTAN

Polisi ini meliputi semua sumber atau aset ICT yang digunakan seperti :

a. Maklumat

i. Semua penyedia perkhidmatan dalam MBK hendaklah mengenal pasti maklumat yang dijana dan hendaklah mengasingkannya mengikut kategori:

1. Maklumat Rahsia Rasmi - Di bawah Akta Rahsia Rasmi 1972 (Akta 88), maksud Maklumat Rahsia Rasmi ialah apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 (Akta 88) dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai "Rahsia Besar", "Rahsia", "Sulit" atau "Terhad" mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972.

2. Maklumat Rasmi - maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh Majlis Bandaraya Kuantan semasa menjalankan urusan rasmi. Maklumat rasmi ini juga merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara.

3. Maklumat Pengenalan Peribadi - Maklumat Pengenalan Peribadi (PII atau *Personally Identifiable Information*) ialah maklumat yang boleh digunakan secara tersendiri atau digunakan bersama maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu. PII boleh juga terkandung dalam Maklumat Rahsia Rasmi.

4. Data Terbuka - Data terbuka merujuk kepada data kerajaan yang boleh digunakan secara bebas, boleh dikongsikan dan digunakan semula oleh rakyat, agensi sektor awam atau swasta untuk sebarang tujuan. PII dikecualikan daripada data terbuka.

b. Aliran Data

i. Aliran data merujuk kepada laluan lengkap data tertentu semasa transaksi. Aliran data dan komunikasi dalam Majlis Bandaraya Kuantan hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Saluran komunikasi termasuk:

1. Saluran komunikasi dan aliran data antara sistem di Majlis Bandaraya Kuantan;
2. Saluran komunikasi dan aliran data ke sistem luar; dan
3. Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.

c. Platform Aplikasi dan Perisian

i. Semua platform aplikasi dan perisian hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

d. Peranti Fizikal dan Sistem

i. Semua peranti fizikal dan sistem hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Peranti fizikal termasuk:

1. Pelayan;
2. Peranti/Peralatan Rangkaian;
3. Komputer Peribadi/Komputer Riba;
4. Telefon/peranti pintar;
5. Media Storan;
6. Peranti dengan sambungan ke rangkaian, contohnya pengimbas, mesin pencetak, sistem kawalan akses, alat kawalan dan sistem kamera litar tertutup (CCTV);
7. Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi Majlis Bandaraya Kuantan; dan
8. Peranti pengesahan *(authentication devices)*, contohnya token keselamatan, *dongle* dan alat pengimbas biometrik.

e. Sistem Luaran

i. Sistem luaran ialah sistem bukan milik Majlis Bandaraya Kuantan yang dihubungkan dengan sistem Majlis Bandaraya Kuantan. Semua sistem luaran hendaklah dikenal pasti, direkodkan dan dinilai tahap keselamatannya secara berkala.

f. Sumber Luaran

i. Semua perkhidmatan sumber luaran hendaklah dikenal pasti, di rekod dan dinilai tahap keselamatannya secara berkala. Perkhidmatan sumber luaran ialah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi Majlis Bandaraya Kuantan. Contoh perkhidmatan sumber luaran ialah:

1. Perisian sebagai satu perkhidmatan
2. Platform sebagai satu perkhidmatan
3. Infrastruktur sebagai satu perkhidmatan
4. Storan pengkomputeran awan
5. Pemantauan keselamatan

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

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

RISIKO

MBK hendaklah mengenal pasti risiko yang berkaitan dengan maklumat yang terlibat. Risiko ialah kebarangkalian Majlis Bandaraya Kuantan tidak dapat melaksanakan fungsi jabatan dengan baik. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam ruang siber MBK.

Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran siber MBK.

Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

a. Kerentanan

Kerentanan adalah kelemahan atau kecacatan aset yang mungkin dieksploitasi dan mengakibatkan pelanggaran keselamatan. Kerentanan setiap aset hendaklah dikenal pasti sebagai sebahagian daripada proses pengurusan risiko.

b. Ancaman

MBK hendaklah mengenal pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

c. Impak

MBK hendaklah menganggarkan impak insiden yang mungkin terjadi. Impak boleh dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi Majlis Bandaraya Kuantan.

d. Tahap Risiko

Tahap risiko ditentukan daripada ancaman, kebarangkalian dan impak risiko. Kaedah penentuan hendaklah mengikut polisi penilaian atau pengurusan risiko yang sedang berkuat kuasa.

e. Penguraian Risiko

Penguraian risiko hendaklah dikenal pasti untuk menentukan sama ada risiko perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/faedahnya.

Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala dengan mengambil kira perkara berikut:

1. Teknologi

Teknologi hendaklah dikenal pasti untuk mengurangkan risiko. Sebagai contoh, tembok api digunakan untuk mengehadkan capaian logikal kepada sistem tertentu.

2. Proses

   Proses *Engineering*, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

3. Manusia

   Mengenal pasti sumber manusia berkelayakan dan kompeten yang mencukupi serta memastikan pengurusan sumber manusia dilaksanakan sebagai pengolahan risiko yang berkesan.

f. Pengurusan Risiko

1. Penyedia perkhidmatan digital di Majlis Bandaraya Kuantan hendaklah memastikan tadbir urus pengurusan risiko diwujudkan dengan mengambil kira perkara berikut:
   i. mengenal pasti kerentanan;
   ii. mengenal pasti ancaman;
   iii. menilai risiko;
   iv. menentukan penguraian risiko;
   v. memantau keberkesanan penguraian risiko; dan
   vi. memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

2. Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya sekali setahun oleh Pasukan Kerja Pelaksana ISMS dan dimaklumkan kepada Mesyuarat Jawatankuasa Audit Dalam ISMS Majlis Bandaraya Kuantan.

PRINSIP KESELAMATAN

Prinsip-prinsip yang menjadi asas kepada PKS MBK dan perlu dipatuhi mengikut kesesuaian maklumat yang dikendalikan adalah seperti berikut:

a. Prinsip "Perlu-Tahu"

MBK hendaklah melaksanakan mekanisme bagi memberikan kebenaran kepada capaian maklumat. Maklumat yang dicapai oleh pengguna yang dibenarkan hendaklah berdasarkan prinsip "Perlu-Tahu" yang membenarkan capaian maklumat yang diperlukan untuk

melaksanakan tugasnya sahaja.

Bagi capaian spesifik Maklumat Rahsia Rasmi, penggunaan yang dibenarkan hendaklah dihadkan kepada masa, lokasi, peranan dan fungsi pengguna tersebut.

b. Hak Keistimewaan minimum

Pengguna hendaklah diberikan hak keistimewaan minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Prinsip ini digunakan untuk menyekat hak akses kepada aplikasi, sistem, proses dan peranti kepada pengguna yang dibenarkan untuk melaksanakan aktiviti. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

c. Pengasingan Tugas

Bagi mengekalkan prinsip sekat-dan-imbang (*check and balance*), Majlis Bandaraya Kuantan hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

d. Kawalan Capaian Berdasarkan Peranan

Capaian sistem hendaklah dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu adalah berdasarkan peranan tersebut.

e. Peminimuman Data

MBK hendaklah mengamalkan prinsip peminimuman data yang mengehadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.

TEKNOLOGI

Teknologi untuk melindungi data hendaklah dikenal pasti di semua peringkat pemprosesan data di setiap elemen pengkomputeran seperti berikut:

a. Peringkat Pemprosesan Data

1. Data-dalam-simpanan

   i. MBK hendaklah menggunakan teknologi yang bersesuaian untukmelindungi data-dalam-simpanan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-simpanan.

   ii. Maklumat Rahsia Rasmi, Maklumat Rasmi dan PII *(Personally Identifiable Information*) perlu dilindungi daripada segi kerahsiaan dan integriti data. Data terbuka perlu dilindungi daripada segi integriti data.

2. Data-dalam-pergerakan

   MBK hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-pergerakan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi datadalam-pergerakan.

3. Data-dalam-penggunaan

   i. MBK hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-penggunaan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Di samping itu, teknologi untuk menentukan asal data dan tanpa sangkalan mungkin diperlukan. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data dalam penggunaan.

   ii. Teknologi yang bersesuaian boleh digunakan untuk memastikan asal data dan data/transaksi tanpa-sangkal.

4. Perlindungan Ketirisan Data

   i. Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.

   ii. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

b. Elemen Dalam Persekitaran Pengkomputeran

Berdasarkan penilaian risiko dan pelan pengurusan risiko, MBK hendaklah menggunakan kaedah teknologi dan kawalan keselamatan (*countermeasure* dan *controlmeasure*) yang dapat melindungi data di semua peringkat saluran pemprosesan bagi semua elemen dalam persekitaran pengkomputeran.

Maklumat Terkawal hendaklah disimpan dan diproses dalam persekitaran pengkomputeran mengikut Prosedur Kawalan Keselamatan Dokumen yang dikeluarkan oleh MBK.

Setiap projek ICT yang dibangunkan di Majlis Bandaraya Kuantan hendaklah mempunyai Pelan Pengurusan Keselamatan Maklumat tersendiri yang mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

1. Peranti pengkomputeran peribadi
   i. Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, stesen kerja, telefon pintar, tablet, dan peranti storan.
   ii. Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Terkawal hendaklah memohon kebenaran daripada pihak bertanggungjawab di Majlis Bandaraya Kuantan. Walau bagaimanapun, peranti pengkomputeran peribadi milik persendirian hendaklah dilarang daripada mencapai Maklumat Terkawal.

2. Peranti rangkaian
   i. Merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti *switch*, *router*, *firewall*, peranti VPN dan kabel.
   ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

3. Aplikasi
   i. Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah *web server*, *server* aplikasi, sistem operasi.
   ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

4. *Server*
    i. *Server* merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat.
    ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

5. Persekitaran fizikal
    i. Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.
    ii. Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip *defence-in-depth*.
    iii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

PROSES

Warga Majlis Bandaraya Kuantan hendaklah melindungi keselamatan siber dengan melaksanakan perkara-perkara berikut:

a. Konfigurasi Asas
   1. Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi prasyarat pentauliahan sistem.
   2. Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan.

b. Kawalan Perubahan Konfigurasi
   1. Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian (*software patch*), pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.
   2. Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asas terkini.
   3. Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan.

c. Backup
   1. *Backup* hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang sedang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan.
   2. Media *backup* hendaklah disimpan dalam persekitaran yang selamat dan di lokasi yang berasingan.

d. Kitaran Pengurusan Aset
   1. Pindah
      i. Pemindahan hak milik aset berlaku dalam keadaan berikut:
         a) Warga Majlis Bandaraya Kuantan meninggalkan agensi disebabkan oleh persaraan, peletakan jawatan atau penugasan semula;
         b) Aset yang dikongsi untuk kegunaan sementara;
         c) Pemberian aset kepada agensi lain; dan
         d) Aset dikembalikan setelah tamat tempoh sewaan.
      ii. Data dalam peranti tersebut hendaklah diuruskan mengikut tatacara pelupusan di perkara (2).

2. Pelupusan
    i. Pelupusan media storan hendaklah dirujuk kepada CGSO sebagai langkah pertama di mana CGSO akan membuat keputusan sama ada sistem itu mengandungi maklumat terperingkat atau sebaliknya.
    ii. Berdasarkan keputusan CGSO, pelupusan perlu dirujuk kepada Arkib Negara Malaysia bagi semakan sama ada sistem itu mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara 2003 (Akta 629) dan Warta Kerajaan P.U.(A)377. Peraturan-Peraturan Arkib Negara (Penetapan Borang-Borang bagi Pelupusan Rekod Awam) 2008.
    iii. Pelupusan boleh dalam bentuk pemusnahan fizikal dan/atau sanitasi data.
    iv. Sanitasi data hendaklah mengikut Garis Panduan Sanitasi Media Elektronik Sektor Awam yang sedang berkuat kuasa.

3. Kitaran Hayat
    i. Kitaran hayat data hendaklah diuruskan mengikut Akta 629.
    ii. Akta 629 memberikan mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umum selama lima tahun.

MANUSIA

Warga Majlis Bandaraya Kuantan, pembekal, pakar runding dan pihak-pihak yang berkepentingan hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

Sistem penyampaian perkhidmatan Kerajaan hendaklah dikendalikan oleh individu yang kompeten dan berpengetahuan. Kakitangan hendaklah dilatih dalam bidang pengkhususan yang diperlukan. Asas kecekapan pengguna hendaklah dibangunkan bagi semua warga Majlis Bandaraya Kuantan.

a. Kompetensi pengguna

1. Kompetensi pengguna termasuk:

   i. Kesedaran amalan terbaik keselamatan maklumat dengan memupuk amalan baik keselamatan siber dengan mewujudkan komunikasi ICT dan program kesedaran keselamatan siber.

   ii. Kemahiran menggunakan alat keselamatan dengan menyediakan latihan yang mencukupi kepada warga Majlis Bandaraya Kuantan berhubung alat-alat keselamatan berkaitan untuk memastikan mereka mampu untuk melaksanakan tugas harian mereka.

   iii. Kompetensi pengguna hendaklah tertakluk kepada penilaian berkala melalui ujian mendalam.

   iv. Setiap orang yang diberi kuasa untuk mengendalikan dokumen berperingkat, kompetensi tambahan pengguna selaras dengan arahan/pekeliling semasa adalah diharapkan.

b. Kompetensi pelaksana

1. Warga Majlis Bandaraya Kuantan yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.
2. Pegawai Keselamatan ICT hendaklah memenuhi syarat-syarat berikut:

   i. Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber.

   ii. Memenuhi keperluan pembelajaran berterusan.

   iii. Menimba pengalaman yang mencukupi dalam bidang keselamatan siber.

   iv. Memperoleh tapisan keselamatan daripada agensi yang diberi kuasa.

3. Pegawai Keselamatan ICT yang dilantik hendaklah memenuhi keperluan kompetensi di atas. Pegawai Keselamatan ICT bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan di Majlis Bandaraya Kuantan.

c. Peranan

1. Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna.
2. Tiada hak capaian automatik diberikan kepada individu tanpa mengiratapisan keselamatan mereka.
3. Warga Majlis Bandaraya Kuantan yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT Jabatan dikembalikan sekiranya berlaku perubahan peranan.
4. Warga Majlis Bandaraya Kuantan yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan yang berkaitan seperti tersenarai dalam senarai aset dalam Nota Serah Tugas.
5. Warga Majlis Bandaraya Kuantan yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan dengan diselia oleh kakitangan yang dipertanggungjawabkan oleh Jabatan

PELAN PENGURUSAN KESELAMATAN MAKLUMAT

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

Pernyataan ini merangkumi perlindungan semua bentuk maklumat elektronik dan bukan elektronik yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan bagi memelihara keselamatan ruang siber dan ketersediaan maklumat 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 dan hanya boleh diubah dengan cara yang dibenarkan.

c. Tidak Boleh Disangkal
   - Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal.

d. Kesahihan
   - Data dan maklumat hendaklah dipastikan kesahihannya.

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

Selain itu, langkah-langkah ke arah memelihara keselamatan siber hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan ICT Majlis Bandaraya Kuantan, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul dan langkah-langkah pencegahan yang perlu diambil untuk menangani risiko berkenaan.

Empat (4) kawalan yang terlibat di dalam Polisi Keselamatan Siber Majlis Bandaraya Kuantan diterangkan dengan lebih jelas dan teratur dalam dokumen ini.

5.0 KAWALAN ORGANISASI *(ORGANIZATIONAL CONTROL)*	
5.1 POLISI KESELAMATAN MAKLUMAT *(POLICIES FOR INFORMATION SECURITY)*	
Menetapkan rangka kerja dasar keselamatan maklumat yang jelas bagi memastikan perlindungan menyeluruh terhadap aset digital dan fizikal MBK daripada sebarang ancaman atau risiko keselamatan.	
KETERANGAN	**PERANAN**
5.1.1 Pelaksanaan Polisi	
Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh Mesyuarat Semakan Pengurusan Majlis Bandaraya Kuantan kepada warga Majlis Bandaraya Kuantan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Majlis Bandaraya Kuantan. Pelaksanaan Polisi ini akan dijalankan oleh Majlis Bandaraya Kuantan dengan disokong oleh Jawatankuasa ISMS terdiri daripada: i) Pengerusi ISMS ii) Pegawai Keselamatan ICT (ICTSO) iii) Ketua-ketua Bahagian iv) Ahli-ahli yang dilantik oleh Majlis Bandaraya Kuantan	Datuk Bandar MBK/ Setiausaha
5.12 Penyebaran Polisi	
Polisi ini perlu disebarkan kepada semua warga MBK dan pihak ketiga termasuklah pembekal, pakar runding dan lain-lain.	ICTSO / Pengarah Jabatan
5.1.3 Penyelenggaraan Polisi	
Polisi Keselamatan Siber ini adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan organisasi. Berikut adalah prosedur yang berkaitan dengan kajian semula Polisi Keselamatan Siber Majlis Bandaraya Kuantan: a. Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan Jawatankuasa ISMS; b. Memaklumkan cadangan pindaan yang telah dipersetujui kepada Jawatankuasa ISMS untuk tujuan pengesahan; c. Memaklumkan perubahan yang telah dipersetujui kepada semua pengguna dalam Mesyuarat Jawatankuasa Pemandu ICT; dan d. Mengkaji semula **sekurang-kurangnya LIMA (5) tahun sekali** ATAU **mengikut keperluan semasa** bagi memastikan dokumen sentiasa relevan.	ICTSO / Jawatankuasa Pemandu ICT / Jawatankuasa ISMS
5.1.4 Pematuhan dan Pengecualian Polisi	
PKS MBK perlu dipatuhi dan terpakai kepada semua warga MBK, Pembekal dan Pihak Ketiga. Tiada pengecualian bagi pematuhan PKS MBK.	Warga MBK / Pembekal / Pihak Ketiga

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBLITIES)*	
Menetapkan peranan dan tanggungjawab yang jelas kepada semua pihak yang terlibat dalam keselamatan maklumat bagi memastikan perlindungan menyeluruh terhadap aset digital dan fizikal MBK.	
KETERANGAN	**PERANAN**
5.2.1 DATUK BANDAR MBK	
Datuk Bandar MBK adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut: a. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah PKS MBK; b. Memastikan semua pengguna mematuhi PKS MBK; c. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; d. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan; dan e. Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JKPICT), MBK.	Datuk Bandar Kuantan
5.2.2 KETUA PEGAWAI MAKLUMAT (CIO) / KETUA PEGAWAI DIGITAL (CDO)	
Peranan dan tanggungjawab CIO/CDO adalah seperti berikut : a. Membantu Datuk Bandar dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT b. Menentukan keperluan keselamatan ICT; c. Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan PKS MBK serta pengurusan risiko dan pengauditan; dan d. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MBK.	Setiausaha MBK
5.2.3 PEGAWAI KESELAMATAN ICT (ICTSO)	
Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini; b. Mengurus keseluruhan program-program keselamatan ICT MBK; c. Menguatkuasakan pelaksanaan PKS MBK; d. Memberi penerangan dan pendedahan berkenaan PKS MBK kepada semua pengguna; e. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS MBK; f. Menjalankan pengurusan risiko; g. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan	Pengarah Bahagian Teknologi Maklumat

MBK berdasarkan hasil penemuan dan menyediakan laporan mengenainya; h. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; i. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; j. Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT Kerajaan (CSIRT), MBK dan ICTSO memaklumkannya kepada CIO/CDO; k. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; dan l. Merancang dan melaksanakan program-program kesedaran mengenai keselamatan ICT. m. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
5.2.4 PENGARAH JABATAN / KETUA BAHAGIAN / KETUA UNIT	
Semua Pengarah Jabatan / Ketua Bahagian / Ketua Unit di Majlis Bandaraya Kuantan berperanan dan bertanggungjawab dalam melaksanakan keperluan Polisi ini dalam operasi semasa Jabatan/Bahagian/Unit seperti yang berikut: a. Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu; b. Pembelian atau peningkatan perisian dan sistem komputer; c. Perolehan teknologi dan perkhidmatan komunikasi baru; d. Menentukan pembekal dan rakan usaha sama menjalani tapisan keselamatan; dan e. Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan dan pelan pengurusan keselamatan maklumat kerajaan yang berkuat kuasa.	Pengarah Jabatan / Ketua Bahagian / Ketua Unit
5.2.5 PENTADBIR SISTEM ICT	
Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;	Pegawai Teknologi Maklumat / Penolong Pegawai Teknologi Maklumat

	b. Mentadbir akaun pengguna; c. Menentukan kawalan akses pengguna terhadap aset ICT MBK; d. Memantau aktiviti capaian sistem aplikasi pengguna; e. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; f. Menganalisis dan menyimpan rekod jejak audit; g. Menyediakan laporan penggunaan sistem secara berkala dan mengikut keperluan; h. Memastikan setiap sistem yang dibangunkan telah dibuat ujian keselamatan; i. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik. j. Melaporkan sebarang insiden keselamatan ICT kepada ICTSO. k. Pengurusan dan pelaksanaan *Accounting & Revenue Integrated System (ARIS)*, termasuk kawalan akses serta capaian pengguna, ditadbir dan diselia oleh pegawai dari Bahagian Teknologi Maklumat	
5.2.6 PENTADBIR TEKNIKAL JABATAN		
Peranan dan tanggungjawab Pentadbir Teknikal Jabatan adalah seperti berikut: a. Pegawai-pegawai jabatan yang dilantik akan menyelaras dan mengurus aplikasi sistem b. Pengurusan keselamatan maklumat		Ketua Bahagian Penolong Pegawai
5.2.7 PENTADBIR RANGKAIAN DAN KESELAMATAN		
Peranan dan tanggungjawab Pentadbir Rangkaian : a. Memantau keadaan rangkaian dan mengawal penggunaan sumber; b. Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) MBK beroperasi sepanjang masa; c. Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna; d. Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; e. Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; dan f. Melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian.		Pegawai Teknologi Maklumat / Penolong Pegawai Teknologi Maklumat

5.2.8 PENTADBIR LAMAN WEB/PORTAL (WEBMASTER)	
Peranan dan tanggungjawab pentadbir Laman Web adalah seperti berikut: a. Menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah; b. Memantau prestasi capaian dan menjalankan *performance tuning* untuk memastikan akses yang lancar; c. Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman; d. Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; e. Melaporkan sebarang pelanggaran keselamatan laman portal kepada ICTSO.	Pegawai Teknologi Maklumat / Penolong Pegawai Teknologi Maklumat
5.2.9 PENTADBIR E-MEL	
Peranan dan tanggungjawab Pentadbir E-Mel adalah seperti berikut: a. Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan Pengarah Jabatan. Pembatalan akaun (pengguna yang berhenti, bertukar, bersara atau melanggar tatacara dan polisi) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; b. Membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib; c. Menyimpan jejak audit selama sekurang-kurangnya enam (6) bulan di dalam pelayan e-mel ATAU tertakluk kepada kemampuan ruang storan; d. Melaksanakan jadual penstoran dan pengarkiban e-mel. Penyimpanan media storan samaada di luar atau di dalam kawasan mestilah mempunyai ciri-ciri keselamatan fizikal yang terjamin bagi mengelak daripada sebarang risiko seperti kehilangan maklumat; e. Memastikan akaun e-mel pengguna sentiasa dalam keadaan baik dan berfungsi; f. Memastikan keselamatan akaun e-mel pengguna dari ancaman luar dan dalam; g. Melaksanakan penyelenggaraan ke atas sistem e-mel dengan baik dan menentukan segala *patches* terkini yang disediakan oleh pihak pembekal dipasang dan berfungsi dengan sempurna; h. Memantau status storan e-mel dan memastikan e-mel Pengurusan Atasan MBK sentiasa tersedia untuk transaksi e-mel; i. Memastikan semua peralatan sistem e-mel sentiasa aktif 24 x 7;	Pegawai Teknologi Maklumat / Penolong Pegawai Teknologi Maklumat

j. Memastikan agar keupayaan *mail relay* hanya boleh digunakan untuk server atau aplikasi dalamn MBK sahaja bagi tujuan keselamatan; k. Memastikan kemudahan membuat capaian e-mel melalui pelbagai media seperti telefon mudah alih disediakan kepada pengguna e-mel MBK; dan l. Memastikan pengguna e-mel MBK berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel MBK dan Internet serta pelaksanaanKursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan melalui latihan serta promosi.	
5.2.10 PEGAWAI ASET ICT	
Peranan dan tanggungjawab pegawai aset ICT adalah seperti berikut: a. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; b. Memastikan Aset ICT milik MBK dilabel dan direkodkan ke dalam Sistem Pengurusan Aset; c. Memastikan Aset ICT milik MBK dibuat pemeriksaan berkala secara tahunan dan di selenggara sebaiknya agar dapat meningkatkan jangka hayat Aset ICT tersebut; d. Memastikan Aset ICT untuk pinjaman dan simpanan sebelum agihan diletakkan di dalam bilikstor yang mempunyai kawalan keselamatan yang terjamin; e. Memastikan Stok alat ganti Aset ICT sentiasa mencukupi dan disimpan di tempat yangselamat dan terkawal; dan f. Memastikan Aset ICT yang ingin dilupuskan dilaksanakan mengikut garis panduan kawalan keselamatan bagi pelupusan data digital.	Pegawai Aset
5.2.11 PENTADBIR PUSAT DATA/BILIK *SERVER* DAN *DISASTER RECOVERY CENTER* (DRC)	
Peranan dan tanggungjawab pegawai adalah seperti berikut : a. Memastikan Operasi Pusat Data/Bilik *Server* dan DRC berada dalam keadaan baik 24 x 7; b. Merancang dan menyelia pelaksanaan simulasi *Disaster Recovery Plan (DRP)* MBK; c. Pengurus operasi DRC sekiranya berlaku bencana terhadap Pusat Data MBK; d. Memastikan Operasi Infrastruktur Virtualisasi di Pusat Data/Bilik *Server* dan DRC berfungsi dan di selenggara dengan baik bagi meningkatkan jangka hayat perkhidmatan perkakasan serta perisian; e. Memastikan Operasi *Backup / Restore* Data berfungsi dan di selenggara dengan baik bagi meningkatkan jangka hayat perkhidmatan perkakasan	Pegawai Teknologi Maklumat / Penolong Pegawai Teknologi Maklumat

serta perisian; f. Memantau Aset ICT sokongan dan Fasiliti Sokongan (*Precision Aircond,* Alat Pencegah Kebakaran, Alarm, Bekalan Elektrik) di Pusat Data/Bilik *Server* dan DRC bagi memastikan beroperasi lancar 24 x 7; g. Menguruskan permohonan baru dan pengemaskinian server dan *Virtual Machine* bagi sistem aplikasi baru di Pusat Data/Bilik *Server* dan DRC; h. Melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian- perisian lain di web server; dan pusat data/bilik *server* dan i. Menguruskan Khidmat Sokongan Operasi Server dari segi Penerimaan, Penyediaan, Penyelenggaraan, Waranti, Pengeluaran dan Pelupusan.	
5.2.12 PENGGUNA	
Peranan dan tanggungjawab pengguna adalah seperti berikut: a. Membaca, memahami dan mematuhi Polisi ini; b. Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya; c. Menjalani tapisan keselamatan sekiranya diperlukan dikehendaki berurusan dengan maklumat rasmi terperingkat; d. Mematuhi prinsip-prinsip Polisi ini dan menjaga kerahsiaan maklumat MBK; e. Melaksanakan langkah-langkah perlindungan seperti berikut :- i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan siber yang ditetapkan; vi. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan bagi setiap langkah-langkah keselamatan siber dari diketahui umum. f. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada Pasukan CSIRT MBK dengan segera; g. Menghadiri program-program kesedaran mengenai keselamatan siber ; dan h. Menandatangani surat akuan pematuhan PKS MBK sebagaimana **LAMPIRAN 1.**	Semua Kakitangan MBK

5.2.13 JURUAUDIT	
Peranan dan tanggungjawab Juruaudit adalah seperti berikut: a. Mengkaji dan menilai kawalan ke atas pematuhan dan pemantauan keselamatan ICT berdasarkan polisi, standard dan prosedur keselamatan maklumat; dan b. Menilai kawalan pengurusan keselamatan aset ICT.	Juruaudit ISMS
5.2.14 JAWATANKUASA PEMANDU ICT MBK (JKPICT)	
Jawatankuasa Pemandu ICT (JKPICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT MBK. Keanggotaan JKPICT MBK adalah seperti berikut: a. Pengerusi : Datuk Bandar MBK b. Ahli : • CIO/CDO MBK • ICTSO MBK • Pengarah-pengarah Jabatan • Pegawai/Penolong Pegawai BTM Bidang kuasa: a. Merangka dasar, hala tuju, garis panduan dan piawaian keselamatan ICT; b. Meneliti, meluluskan dan menguatkuasakan Polisi Keselamatan Siber; c. Meneliti dan meluluskan program dan aktiviti yang berkaitan dengan keselamatan ICT; d. Memastikan peruntukan kewangan yang mencukupi disediakan untuk pelaksanaan program dan aktiviti keselamatan ICT; e. Meneliti dan meluluskan inisiatif untuk peningkatan keselamatan ICT; f. Memantau ancaman-ancaman utama terhadap aset-aset ICT; dan	Ahli JKPICT MBK
5.2.15 PASUKAN TINDAK BALAS INSIDEN KESELAMATAN SIBER MBK (CSIRT)	
Keanggotaan CSIRT MBK adalah seperti berikut: Pengurus : CDO Penolong Pengurus : ICTSO Ahli : a) Pegawai Teknologi Maklumat BTM b) Penolong Pegawai Teknologi Maklumat BTM	Pasukan CSIRT MBK

Peranan dan tanggungjawab CSIRT MBK adalah seperti berikut: a. Menerima dan mengesan aduan keselamatan siber serta menilai tahap dan jenis insiden; b. Merekod dan menjalankan siasatan awal insiden yang diterima; c. Menangani tindak balas (*response*) insiden keselamatan siber dan mengambil tindakan baik pulih minimum; d. Menghubungi dan melaporkan insiden yang berlaku kepada ICTSO dan pihak NACSA sama ada sebagai input atau untuk tindakan seterusnya; e. Menasihati pengguna dengan mengambil tindakan pemulihan dan pengukuhan; f. Menyebarkan makluman berkaitan pengukuhan keselamatan siber CSIRT MBK kepada pengguna MBK; dan g. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
5.3 PENGASINGAN TUGAS (*SEGREGATION OF DUTIES*)	
Memastikan tugas-tugas kritikal dalam pengurusan sistem dan maklumat dipisahkan secara berstruktur bagi mengurangkan risiko penyelewengan, akses tanpa kebenaran, dan kesilapan operasi.	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan c. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai "*production*". Pengasingan juga merangkumi tindakan memisahkan antara kumpulan	ICTSO / Pegawai Teknologi Maklumat / Penolong Pegawai Teknologi Maklumat
5.4 TANGGUNGJAWAB PENGURUSAN *(MANAGEMENT RESPONSIBILITIES)*	
Memastikan pengurusan atasan bertanggungjawab sepenuhnya terhadap pelaksanaan, pemantauan dan pematuhan dasar keselamatan maklumat serta menyokong budaya keselamatan dalam organisasi.	
1. Memastikan kakitangan dan pembekal memahami dan mematuhi perundangan, Arahan Perkhidmatan, peraturan dan PKS MBK, 2. Memastikan kakitangan dan pembekal mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh MBK.	Pihak Pengurusan

5.5 HUBUNGAN DENGAN PIHAK BERKUASA (*CONTACT WITH AUTHORITIES*)	
Memastikan MBK mempunyai saluran hubungan yang jelas dan rasmi dengan pihak berkuasa berkaitan bagi pelaporan, pematuhan, serta kerjasama dalam isu-isu keselamatan maklumat dan insiden siber.	
Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab MBK; b. Mewujudkan dan mengemas kini prosedur / senarai pihak berkuasa perundangan / pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia dan Suruhanjaya Komunikasi Dan Multimedia Malaysia. Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta Bomba; dan c. Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden dan tidak berkompromi kepada sebarang aktiviti pelanggaran	CSIRT MBK
5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS *(CONTACT WITH SPECIAL INTEREST GROUPS)*	
Memastikan MBK menjalin hubungan yang berterusan dengan kumpulan berkepentingan khas dalam bidang keselamatan maklumat bagi mendapatkan maklumat semasa, amalan terbaik dan sokongan teknikal.	
Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau forum bagi: a. Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat; b. Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini; c. Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan;dan d. Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	Pihak perunding / agensi
5.7 ANCAMAN PERISIKAN *(THREAT INTELLIGENCE)*	
Untuk membolehkan MBK mengenal pasti, menilai dan bertindak balas terhadap ancaman keselamatan maklumat secara proaktif melalui penggunaan maklumat perisikan ancaman yang sah dan terkini.	
Teknologi Maklumat dan Komunikasi (ICT) merujuk kepada rangkaian langkah dan tindakan yang diambil untuk mengesan, melindungi, dan mencegah pelbagai jenis ancaman perisikan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Sistem Pemantauan (*Security Monitoring*): Mengesan aktiviti mencurigakan atau sebarang ancaman perisikan yang mungkin berlaku dalam rangkaian atau sistem.	ICTSO / Pegawai Teknologi Maklumat / Penolong Pegawai Teknologi Maklumat

b. Pendinding Api (*Firewall*): Memasang firewall bagi mengawal trafik rangkaian daripada aktiviti yang mencurigakan. c. Enkripsi Data (*Encryption*): Semua data yang disimpan hendaklah dienkripsi bagi melindunginya daripada diakses oleh pihak yang tidak sah. d. Kemaskini Perisian: Memastikan semua perisian yang digunakan adalah versi terkini dan sentiasa dikemas kini. e. Kawalan Akses Pengguna: Akses pengguna kepada aplikasi sistem hendaklah dikawal berdasarkan skop tugas yang telah ditetapkan oleh Jabatan/Bahagian.	
5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK *(INFORMATION SECURITY IN PROJECT MANAGEMENT)*	
Memastikan bahawa aspek keselamatan maklumat diambil kira secara menyeluruh dalam setiap peringkat pelaksanaan projek ICT di MBK.	
Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek di MBK; b. Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek; c. Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan; dan d. Dokumen kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam PKS MBK; dan e. Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal yang mempunyai pensijilan keselamatan maklumat (mengikut keperluan)	Warga MBK (Pasukan Projek)
5.9 MAKLUMAT INVENTORI ASET DAN YANG BERKAITAN *(INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS)*	
Memastikan semua aset maklumat dan aset berkaitan dikenal pasti, direkod, dikawal serta dilindungi mengikut tahap kepentingannya kepada operasi dan keselamatan organisasi.	
1. Memastikan semua aset ICT MBK hendaklah disokong dan diberi perlindungan yang bersesuaian. 2. Perkara yang perlu dipatuhi adalah seperti berikut : a. Mengenal pasti Pegawai Penerima Aset setiap Bahagian untuk menguruskan penerimaan aset-aset ICT bagi projek-projek ICT; b. Memastikan semua aset ICT dikenalpasti, di klasifikasi, di dokumen, diselenggara dan dilupuskan. Maklumat aset direkodkan dan sentiasa dikemaskini sebagaimana arahan dan peraturan yang berkuatkuasa dari semasa ke semasa;	Pegawai Aset / Warga MBK

c. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; d. Pegawai Aset hendaklah mengesahkan penempatan aset ICT; e. Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti,di dokumen dan dilaksanakan; dan f. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICTdi bawah kawalannya. 3. Aset ICT yang di selenggara hendaklah milik MBK. Perkara yang perlu dipatuhi oleh pemilik aset adalah seperti berikut : a. Memastikan aset ICT di bawah tanggungjawabnya telah dimasukkan dalam senarai aset; b. Memastikan aset ICT telah dikelaskan dan dilindungi; c. Mengenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan; d. Memastikan pengendalian aset ICT dilaksanakan dengan baik apabila aset di hapus atau dilupuskan; dan e. Memastikan semua jenis aset dipelihara dengan baik.	
5.10 PENGGUNAAN YANG DIBENARKAN BAGI MAKLUMAT DAN ASET YANG BERKAITAN *(ACCEPTABLE USE OF INFORMATION AND OTHER ASSOCIATED ASSETS)*	
Memastikan semua pengguna memahami dan mematuhi garis panduan penggunaan yang dibenarkan bagi aset maklumat dan aset ICT MBK untuk melindungi kerahsiaan, integriti dan ketersediaan sistem dan data.	
5.10.1 Pemilikan Aset	
Memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja.	Pegawai Aset / Warga MBK
5.10.2 Kepenggunaan Aset yang Dibenarkan	
Peraturan untuk penggunaan aset mengikut kaedah atau polisi kepenggunaan yang dibenarkan dan aset yang berhubung kait dengan maklumat dan kemudahan memproses maklumat perlu dikenal pasti, direkodkan dan dilaksanakan. Peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan.	Warga MBK
5.11 PEMULANGAN ASET (*RETURN OF ASSETS*)	
Memastikan semua aset maklumat dan aset ICT yang dibekalkan kepada pengguna dipulangkan dengan selamat dan lengkap apabila perkhidmatan atau tanggungjawab mereka tamat, ditukar atau tidak lagi memerlukan penggunaan aset tersebut.	
1. Warga MBK dan pihak lain yang berkepentingan, mengikut kesesuaian, hendaklah memulangkan semua aset milik MBK dan menandatangani borang penerimaan aset ICT dalam penggunaan mereka selepas pertukaran atau penamatan pekerjaan atau kontrak. 2. Pemilik aset hendaklah memastikan semua aset ICT yang diserahkan kepadanya dikembalikan kepada Bahagian Teknologi Maklumat selepas	Pegawai Aset / BTM / Warga MBK

penamatan pekerjaan atau kontrak. 3. Bahagian Teknologi Maklumat hendaklah merekodkan maklumat pulangan aset. 4. Aset ICT yang mengandungi maklumat MBK hendaklah dilupuskan dengan selamat sebelum menyerah semula aset berkenaan kepada Bahagian Teknologi Maklumat.	
5.12 PENGELASAN MAKLUMAT (*CLASSIFICATION OF INFORMATION)*	
Memastikan maklumat diklasifikasikan mengikut tahap sensitiviti dan kepentingannya bagi menjamin kerahsiaan, integriti dan ketersediaannya daripada sebarang ancaman atau akses tidak sah.	
1. Maklumat dan dokumen hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. 2. Dokumen Rasmi Kerajaan dibahagikan kepada dua (2), iaitu : i. Terperingkat : Setiap maklumat yang dikelaskan sebagai terperingkat mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: • Rahsia Besar; • Rahsia; • Sulit; atau • Terhad dan ii. Terbuka: Pengurusan dokumen ini tidak tertakluk kepada peraturan dokumen terperingkat.	Pengarah Jabatan / Ketua Bahagian / Pegawai Tadbir
5.13 PELABELAN MAKLUMAT *(LABELLING OF INFORMATION)*	
Memastikan maklumat yang diklasifikasikan dilabel dengan jelas dan konsisten bagi memudahkan pengendalian, penyimpanan dan pemindahan maklumat mengikut tahap keselamatan yang ditetapkan.	
1. Pelabelan maklumat mestilah selaras dengan skim klasifikasi maklumat di MBK 2. Maklumat hendaklah dilabelkan dengan sewajarnya mengikut buku Arahan Keselamatan.	Pengarah Jabatan / Ketua Bahagian / Pegawai Teknologi Maklumat
5.14 PEMINDAHAN MAKLUMAT *(INFORMATION TRANSFER)*	
Memastikan pemindahan maklumat, sama ada secara dalaman atau luaran, dilakukan dengan selamat, teratur dan mematuhi dasar keselamatan serta peraturan berkaitan.	
Memastikan keselamatan pertukaran maklumat dan perisian antara MBK dan agensi luar terjamin. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penghantaran atau pemindahan maklumat perlulah mendapat kebenaran daripada pemilik terlebih dahulu. b. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara MBK dengan agensi luar;	Pentadbir Sistem

c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MBK; dan d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	
5.14.1 Keselamatan Dokumen	
Melindungi maklumat MBK dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian. Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Menyedia dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	Pentadbir Sistem
5.14.2 Pelupusan Dokumen	
Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan Menggunakan inskripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan sekiranya dihantar secara elektronik.	Pegawai Aset
5.14.3 Perjanjian Dalam Pemindahan Maklumat	
Perjanjian untuk pemindahan maklumat sama ada secara elektronik atau cetakan di antara MBK dan pihak luar perlu dilaksanakan mengikut keperluan dan ianya perlu dilakukan bergantung kepada tahap sensitiviti sesuatu maklumat yang dikendalikan.	Pentadbir Sistem / Pentadbir Teknikal
5.14.4 Mesej Elektronik	
1. Maklumat yang terkandung di dalam mesej elektronik perlu dilindungi. Penggunaan mesej elektronik hanya boleh digunakan untuk aktiviti kerja harian di mana penggunaan untuk kepentingan peribadi hendaklah dilarang bagi mengelakkan daripada sebarang bentuk gangguan dan ancaman kepada keselamatan maklumat. 2. Penggunaan e-mel di MBK hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan” dan mana-mana undang-undang bertulis yang berkuat kuasa. 3. Penguatkuasaan kuota saiz inbox ditetapkan seperti berikut : a. Pengurusan Tertinggi : 100GB b. Ahli Majlis : 5GB	Pentadbir Sistem / Pentadbir Teknikal

c. Pengurusan Dan Profesional : 100GB d. Sokongan B : 100GB e. Sokongan C : 100GB f. Sokongan D : 5GB Permohonan saiz inbox emel yang lebih besar boleh dipohon melalui Bahagian Teknologi Maklumat. 4. Tindakan penguatkuasaan kuota saiz emel melibatkan perkara - perkara berikut ; a. Had saiz inbox bagi setiap kakitangan; b. Padam emel lama yang tidak lagi diperlukan, terutamanya emel dengan lampiran besar. c. Kosongkan folder “Deleted Items”, “Sent Items”, dan “Junk Email” secara berkala. d. Laksanakan semakan berkala (email housekeeping) sekurang-kurangnya sekali sebulan bagi memastikan akaun emel sentiasa berada di bawah had kouta yang ditetapkan. e. Pantau amaran penggunaan kouta yang dihantar oleh sistem bagi mengelakkan gangguan penghantaran atau penerimaan emel. 5. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh MBK sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh MBK; b. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; c. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; d. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; e. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; f. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; g. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; h. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; i. Pengguna hendaklah menentukan tarikh dan masa sistem komputer	Warga MBK

adalah tepat; j. Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; k. Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my, hotmail.com dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; kecuali jika e-mel rasmi menghadapi masalah; l. Pengguna hendaklah bertanggung jawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing. m. Akaun e-mel kakitangan yang berhenti atau tamat perkhidmatan perlu dilupuskan sekurang-kurangnya 1 bulan dari tarikh akhir berkhidmat.	
5.14.5 Perjanjian Kerahsiaan atau Ketidakkritisan Maklumat	
Keperluan bagi perjanjian kerahsiaan atau ketidakkritisan maklumat yang mencerminkan keperluan organisasi untuk melindungi maklumat perlu dikenal pasti, dikaji secara berkala jika perlu dan didokumenkan.	Pentadbir Sistem / Pentadbir Teknikal
5.15 KAWALAN AKSES (*ACCESS CONTROL*)	
Memastikan hanya individu yang sah, dibenarkan dan diberi kuasa mempunyai akses kepada sistem, rangkaian, maklumat dan aset ICT MBK mengikut tahap keperluan tugas (*need-to-know basis*).	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu diwujudkan, didokumenkan, dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini setahun sekali atau mengikut keperluan dan menyokong peraturan kawalan capaian sedia ada. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Keperluan keselamatan aplikasi; b. Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian; c. Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa; d. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; e. Pengasingan peranan kawalan capaian; f. Kebenaran rasmi permintaan akses; g. Keperluan semakan hak akses berkala; h. Pembatalan hak akses; i. Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat;dan j. Capaian *privilege.* Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari MBK. Kawalan	Pemilik dan Pentadbir Sistem / Pentadbir Teknikal

capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Memastikan hanya pengguna yang dibenarkan sahaja boleh mendapat perkhidmatan rangkaian; b. Menempatkan, mengasingkan atau memasang peralatan ICT yang bersesuaian untuk kawalan keselamatan antara rangkaian Majlis Bandaraya Kuantan, rangkaian agensi lain dan rangkaian awam; dan c. Mewujud, menguatkuasakan dan memantau mekanisme untuk pengesahan pengguna, ID pengguna, kata laluan atau peralatan ICT yang dihubungkan ke rangkaian termasuk rangkaian tanpa wayar. d. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	
5.16 PENGURUSAN IDENTITI (*IDENTITY MANAGEMENT)*	
Memastikan setiap pengguna sistem ICT MBK dikenal pasti secara unik dan mempunyai kawalan ke atas identiti mereka untuk mengelakkan capaian yang tidak dibenarkan.	
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara-perkara berikut hendaklah dipatuhi : a. Akaun yang diperuntukkan oleh MBK sahaja boleh digunakan; b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c. Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan MBK. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f. Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Bertukar bidang tugas kerja; ii. Bertukar ke agensi lain; iii. Bersara; atau iv. Ditamatkan perkhidmatan	Pengguna / Warga MBK

5.17 MAKLUMAT PENGESAHAN *(AUTHENTICATION INFORMATION)*	
Melindungi maklumat pengesahan seperti kata laluan, PIN, token dan data biometrik bagi memastikan hanya pengguna yang sah boleh mengakses sistem dan maklumat ICT MBK.	
Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan menggunakan kawalan pengesahan maklumat seperti penyulitan (*encryption*) atau *two-factor authentication* (2-FA) atau *multi-factor authentication* (MFA)	Pentadbir Sistem ICT / Warga MBK
5.18 HAK AKSES (*ACCESS RIGHT*)	
Memastikan capaian kepada sistem dan maklumat ICT MBK hanya diberikan kepada individu yang diberi kuasa, mengikut keperluan tugas dan tahap keselamatan yang sesuai.	
Hak akses pengguna kepada maklumat dan aset berkaitan hendaklah diperuntukkan, disemak dan diubahsuai mengikut keperluan organisasi dan prosedur kawalan akses. Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan, b. Akaun pengguna mestilah unik, c. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu, d. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan, e. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang, dan f. Pentadbir Sistem ICT akan membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Bertukar bidang tugas kerja; ii. Bertukar ke agensi lain; iii. Bersara; atau iv. Ditamatkan perkhidmatan. v. Tertakluk kepada arahan dan makluman dari Jabatan Khidmat Pengurusan.	Pentadbir Sistem ICT Pentadbir Teknikal Warga MBK
5.19 HUBUNGAN KESELAMATAN MAKLUMAT DENGAN PEMBEKAL *(INFORMATION SECURITY IN SUPPLIER RELATIONSHP)*	
Menetapkan garis panduan dan kawalan keselamatan maklumat dalam semua hubungan dengan pembekal, kontraktor, vendor dan pihak ketiga yang mempunyai akses kepada maklumat, sistem atau aset MBK.	
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset MBK. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Mengenalpasti dan mendokumentasi jenis pembekal mengikut kategori;	ICTSO/BTM Pemilik Projek Bahagian Perolehan Pihak Ketiga/Pembekal

b. Proses kitaran hayat (*lifecycle*) yang seragam untuk menguruskan pembekal; c. Mengawal dan memantau akses pembekal; d. Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian; e. Jenis-jenis obligasi kepada pembekal; f. Melaksanakan program kesedaran terhadap PKS MBK kepada pembekal; g. Menandatangani Surat Perakuan Pematuhan Akta Rahsia Rasmi 1972 Dan Polisi Keselamatan Siber Majlis Bandaraya Kuantan (LAMPIRAN 3); dan h. Pembekal perlu mematuhi arahan keselamatan yang berkuatkuasa.	
5.20 KESELAMATAN MAKLUMAT DALAM PERJANJIAN DENGAN PEMBEKAL *(ADDRESSING INFORMATION SECURITY WITHIN SUPPLIER AGREEMENTS)*	
Menetapkan keperluan untuk memasukkan kawalan keselamatan maklumat dalam semua perjanjian, kontrak, dan memorandum persefahaman dengan pembekal, kontraktor, vendor, atau pihak ketiga.	
Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi. Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak MBK selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa. Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak MBK mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. MBK hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan; b. Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan; c. Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan; d. Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; e. Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal;	Pegawai Teknologi Maklumat/ Penolong Pegawai Teknologi Maklumat Akauntan/ Pegawai Undang-Undang/ Syarikat Pembekal

f. Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut: a. Badan penilai pihak ketiga adalah bebas dan berintegriti; b. Badan penilai pihak ketiga adalah kompeten; c. Kriteria penilaian; d. Parameter pengujian; dan e. Andaian yang dibuat berkaitan dengan skop penilaian. g. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan MBK; dan h. Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh MBK.	
5.21 PENGURUSAN KESELAMATAN MAKLUMAT DALAM RANTAIAN BEKALAN TEKNOLOGI KOMUNIKASI ICT *(MANAGING INFORMATION SECURITY IN THE INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SUPPLY CHAIN)*	
Menetapkan kawalan keselamatan maklumat dalam semua aktiviti perolehan, penggunaan, penyelenggaraan, dan pelupusan aset ICT bagi memastikan risiko keselamatan dalam rantaian bekalan dapat diminimumkan.	
Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: a. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b. Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada sub kontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembelian produk; dan c. Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	Pegawai Teknologi Maklumat/ Penolong Pegawai Teknologi Maklumat/ Pegawai Undang-Undang/ Syarikat Pembekal
5.22 PEMANTAUAN, KAJIAN SEMULA DAN PENGURUSAN PERUBAHAN PERKHIDMATAN PEMBEKAL *(MONITORING, REVIEW AND CHANGE MANAGEMENT OF SUPPLIER SERVICES)*	
Menetapkan garis panduan bagi memastikan semua perkhidmatan yang dibekalkan oleh pembekal sentiasa mematuhi keperluan keselamatan maklumat MBK, melalui pemantauan berterusan, kajian semula prestasi dan pengurusan perubahan yang terkawal.	
Prestasi perkhidmatan pembekal hendaklah sentiasa dipantau, diaudit dan dikaji semula secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: a. Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; b. Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan	Pegawai Teknologi Maklumat/ Penolong Pegawai Teknologi Maklumat/ Pegawai Undang-Undang/ Syarikat Pembekal

c. Memaklumkan mengenai insiden keselamatan kepada pembekal, pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian Perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor. Perkara yang perlu diambil kira adalah seperti berikut: a. Perubahan dalam perjanjian dengan pembekal; b. Perubahan yang dilakukan oleh MBK bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan c. Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	
5.23 KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN *AWAN* *(INFORMATION SECURITY FOR USE OF CLOUD SERVICES)*	
Menetapkan garis panduan dan kawalan keselamatan maklumat bagi penggunaan perkhidmatan awan (*cloud services*) oleh MBK untuk memastikan perlindungan data, pematuhan undang-undang dan kawalan akses yang selamat.	
Perkhidmatan awan adalah penting untuk memastikan bahawa organisasi memilih penyedia perkhidmatan awam yang mempunyai tahap keselamatan yang tinggi. Berikut adalah beberapa langkah-langkah yang diperlukan sebelum penggunaan perkhidmatan awan. a. Menetapkan skop perolehan perkhidmatan awan yang ingin dikawal. Skop ini perlu merangkumi jenis perkhidmatan awan yang diperlukan, data yang akan dipindahkan ke awan, dan syarat-syarat keselamatan yang dikehendaki. b. Memilih penyedia perkhidmatan awan yang mematuhi piawaian keselamatan maklumat dan memiliki rekod prestasi yang baik dalam bidang keselamatan dan privasi data. c. Membuat perjanjian perkhidmatan dengan penyedia perkhidmatan awan yang mencakup butiran keselamatan maklumat, seperti tahap layanan, perlindungan data, pematuhan piawaian, pemisahan data, pemulihan bencana, dan peraturan pematuhan. d. Melakukan audit keselamatan secara berkala ke atas penyedia perkhidmatan awan untuk memastikan pematuhan mereka terhadap perjanjian perkhidmatan dan piawaian keselamatan maklumat. e. Memastikan bahawa penyedia perkhidmatan awan mempunyai perancangan pemulihan bencana yang kukuh untuk melindungi data organisasi dalam kejadian insiden yang merugikan.	ICTSO BTM Pentadbir Rangkaian

f. Menilai semula keselamatan maklumat secara berkala dan memastikan ia selaras dengan keperluan keselamatan dan piawaian. g. Memastikan bahawa organisasi mematuhi peraturan dan perundangan yang berkaitan dengan penggunaan perkhidmatan awan, terutamanya dalam hal privasi data dan perlindungan data peribadi.	
5.24 PERANCANGAN DAN PERSEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY INCIDENT MANAGEMENT PLANNING AND PREPARATION)*	
Menetapkan panduan perancangan dan penyediaan yang sistematik untuk mengurus insiden keselamatan maklumat, bagi memastikan tindak balas yang pantas, berkesan dan meminimumkan kesan kepada operasi MBK.	
5.24.1 Tanggungjawab dan Prosedur	
Prosedur pelaporan insiden keselamatan siber perlu dilaksanakan berdasarkan Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam.	Pasukan CSIRT MBK
5.24.2 Melaporkan Peristiwa Keselamatan Maklumat	
1. Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar polisi keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. 2. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan CSIRT MBK dengan kadar segera: a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. f. Sistem Aplikasi kerap kali atau berulang kali mengalami masalah tidak berfungsi dan sebagainya	CIO/CDO ICTSO BTM Warga MBK
5.24.3 Melaporkan Kelemahan Keselamatan Maklumat	
Pelaporan juga perlu dilakukan sekiranya terdapat kelemahan keselamatan di dalam sistem atau perkhidmatan. Pelaporan insiden keselamatan ICT kepada pihak pengurusan hendaklah melalui Mesyuarat Pemandu ICT (JPICT) atau mesyuarat pengurusan yang setaraf.	Pasukan CSIRT MBK / Warga MBK

5.25 PENILAIAN DAN KEPUTUSAN PERISTIWA KESELAMATAN MAKLUMAT ***(ASSESSMENT AND DECISION ON INFORMATION SECURITY EVENTS)***	
Menetapkan panduan bagi mengenal pasti, menilai, dan membuat keputusan yang tepat terhadap peristiwa keselamatan maklumat (*information security events*) supaya ia dapat ditangani secara berkesan sebelum berkembang menjadi insiden keselamatan yang serius.	
Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.	Pasukan CSIRT MBK
5.26 MAKLUMBALAS INSIDEN KESELAMATAN MAKLUMAT ***(RESPON TO INFORMATION SECURITY INCIDENT)***	
Memastikan tindak balas yang efisien dan efektif kepada insiden keselamatan maklumat.	
Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT Majlis Bandaraya Kuantan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut: a. Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; b. Menjalankan kajian forensik sekiranya perlu; c. Menghubungi pihak yang berkenaan dengan secepat mungkin; d. Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti; e. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; f. Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; g. Menyediakan tindakan pemulihan segera; dan h. Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	Pasukan CSIRT MBK
5.27 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT ***(LEARNING FROM INFORMATION SECURITY INCIDENTS)***	
Mengurangkan kebarangkalian atau kesan daripada insiden akan datang.	
Pengetahuan yang diperoleh daripada penganalisisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya. Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah.	Pasukan CSIRT MBK

5.28 PENGUMPULAN BAHAN BUKTI *(COLLECTION OF EVIDENCE)*	
Memastikan pengurusan bukti yang konsisten dan efektif berkaitan dengan insiden keselamatan maklumat bagi tujuan tindakan disiplin dan undang-undang.	
Bahan-bahan bukti berkaitan insiden keselamatan siber hendaklah direkod, disimpan dan dikemaskini. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut : a. Menyimpan jejak audit, penduaan secara berkala dan melindungi integriti semua bahan bukti, b. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan, c. Menyediakan pelan kontingensi dan mengaktifkan pelan pemulihan bencana, d. Menyediakan tindakan pemulihan segera, dan e. Memaklumkan atau mendapatkan nasihat pihak berkuasa berkaitan perundangan sekiranya perlu.	Pasukan CSIRT MBK
5.29 MELAKSANAKAN KESINAMBUNGAN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY DURING DISRUPTION)*	
Memastikan bahawa walaupun operasi terganggu, risiko pendedahan data atau kerosakan maklumat dapat diminimumkan dan perkhidmatan dapat dipulihkan dengan cepat serta selamat.	
Pelan Kesinambungan Perkhidmatan atau Pelan Pemulihan Bencana hendaklah dilaksanakan mengikut keperluan semasa bagi menentukan agar suatu pendekatan yang menyeluruh dapat diambil bagi mengekalkan kesinambungan perkhidmatan. Ini juga bertujuan untuk memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan MBK dan menjamin keselamatan maklumat ICT MBK.	ICTSO / Pasukan DRP
5.30 KETERSEDIAAN ICT UNTUK KESINAMBUNGAN PERKHIDMATAN *(ICT READINESS FOR BUSINESS CONTINUITY)*	
Memastikan maklumat dan aset ICT MBK tersedia apabila berlaku gangguan. Ketersediaan ICT hendaklah dirancang, dilaksana, diselenggara dan diuji berdasarkan objektif kesinambungan perkhidmatan dan keperluan kesinambungan ICT.	
Teknologi Maklumat dan Komunikasi (ICT) adalah aspek penting dalam memastikan kesinambungan operasi organisasi. Ini melibatkan penyediaan infrastruktur, sistem, dan perkhidmatan ICT yang boleh di akses dan berfungsi dengan baik dalam semua keadaan, termasuk semasa krisis atau gangguan. Faktor-faktor yang perlu dipertimbangkan untuk mencapai ketersediaan ICT bagi kesinambungan organisasi adalah seperti berikut : a. Organisasi perlu mempunyai perancangan strategik ICT yang jelas dan menyeluruh yang mengenal pasti keperluan teknologi bagi menjayakan strategi kesinambungan perniagaan.	ICTSO / Pasukan DRP / Pentadbir Rangkaian / Pentadbir Sistem

b. Ini termasuk menentukan sumber daya ICT yang diperlukan, tujuan pemulihan, dan kebijakan perolehan peralatan dan perkhidmatan c. Mempunyai infrastruktur ICT yang *redundant*, termasuk rangkaian, pelayan, storan data, dan sokongan kuasa yang boleh berfungsi jika ada gangguan atau kegagalan. d. Penggantian secara automatik (*failover*) dan peralatan cadangan perlu dipertimbangkan. e. Lakukan pemantauan aktif terhadap peralatan ICT untuk mengenal pasti masalah sebelum ia berlaku dan mengelakkan gangguan. f. Pengurusan inventori peralatan, pelan pembaikan, dan pemantauan prestasi berterusan. g. Sediakan pelan pemulihan bencana ICT yang komprehensif. Ini termasuk cadangan data, pengekalan cadangan pelayan, dan prosedur pemulihan semula aktiviti perniagaan. h. Ujian dan latihan berkala pelan pemulihan bencana. i. Pastikan akses kepada sistem dan data dikawal dengan ketat dan disemak secara berkala. Ini termasuk pengurusan identiti, pengesahan dua faktor (2fa), dan peraturan akses yang ketat. j. Sediakan perkhidmatan pengurusan keselamatan seperti antivirus, *firewall*, dan pelindung kegagalan untuk menghalang ancaman keselamatan ICT. k. Amalkan pemantauan keselamatan untuk mengenal pasti dan tindak balas kepada ancaman dan insiden keselamatan. l. Pastikan kakitangan tahu apa yang perlu dilakukan dalam kes insiden keselamatan. m. Melaksanakan penyelenggaraan dan pembaikan peralatan dan sistem secara berkala untuk mengelakkan kegagalan yang tidak dijangka. n. Tetapkan jadual pembaikan berkala dan pemulihan data. o. Pantau penggunaan sumber daya ICT seperti *bandwidth* dan kapasiti penyimpanan untuk mengelakkan penggunaan berlebihan yang boleh menyebabkan gangguan. p. Pastikan penyedia perkhidmatan awan atau penyedia perkhidmatan lain mempunyai pelan kesinambungan perniagaan yang mencukupi yang dapat menyokong operasi anda jika berlaku gangguan.	

5.31 KEPERLUAN PERUNDANGAN, STATUTORI, KAWAL SELIA DAN KONTRAKTUAL *(LEGAL, STATUTORY, REGULATORY ANDCONRACTUAL REQUIREMENTS)*	
Untuk memastikan bahawa semua aktiviti berkaitan keselamatan maklumat mematuhi undang-undang dan peraturan yang berkaitan, serta memenuhi tanggungjawab perjanjian kontrak dengan pihak dalaman dan luaran.	
Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga MBK, pembekal, pakar runding dan pihak yang menggunakan perkhidmatan digital MBK. Keperluan perundangan atau pertaturan-peraturan lain berkaitan yang perlu dirujuk oleh semua pengguna di MBK dan pembekal seperti di LAMPIRAN 5. Pekerja hendaklah mematuhi keperluan perundangan, kawal selia dan kontrak yang berkaitan dengan hak harta intelek dan penggunaan produk perisian proprietari. (contoh: Microsoft Office) Pekerja bertanggungjawab untuk melindungi rekod daripada kehilangan, kemusnahan, pemalsuan, capaian tanpa kebenaran dan pelepasan tanpa kebenaran, selaras dengan keperluan perundangan, kawal selia, kontrak dan perniagaan.	Warga MBK / Pembekal / Pakar Runding / Pihak yang mengakses dan menggunakan perkhidmatan MBK
5.32 HAK HARTA INTELEK *(INTELLECTUAL PROPERTY RIGHTS)*	
Melindungi hak harta intelek MBK dan memastikan semua penggunaan, pembangunan serta pengedaran perisian, sistem dan dokumen mematuhi undang-undang serta etika harta intelek.	
MBK hendaklah memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian yang berkaitan hak harta intelektual. Penggunaan perisian berlesen hendaklah dikuatkuasakan bagi memastikan pematuhan undang-undang, mengemaskini penyelenggaraan dan naik taraf perisian, meningkatkan keselamatan perisian dan membantu mengekalkan hubungan positif dengan pembekal perisian.	Warga MBK / Pembekal / Pakar Runding / Pihak yang mengakses dan menggunakan perkhidmatan MBK
5.33 PERLINDUNGAN REKOD *(PROTECTION OF RECORDS)*	
Memastikan semua rekod yang dimiliki, dikawal dan diproses oleh MBK dilindungi daripada kehilangan, kerosakan, akses tanpa kebenaran atau pindaan yang tidak sah sepanjang kitar hayatnya.	
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian tanpa kebenaran dan pelepasan tanpa kebenaran. Semua pihak dalaman dan luaran, termasuk kakitangan MBK yang mempunyai capaian kepada maklumat MBK atau terlibat dalam proses kerja MBK perlu mematuhi PKS MBK dan undang-undang, peraturan dan keperluan kontrak berkenaan.	Warga MBK / Pembekal / Pakar Runding / Pihak yang mengakses dan menggunakan perkhidmatan MBK

5.34 PRIVASI DAN PERLINDUNGAN MAKLUMAT PERIBADI BOLEH DIKENAL PASTI *(PRIVACY AND PROTECTION OF PERSONAL IDENTIFIABLE INFORMATION - PII)*	
Menjamin bahawa semua maklumat peribadi yang dikendalikan oleh organisasi adalah selamat, sulit, dan digunakan hanya untuk tujuan yang dibenarkan, bagi mengelakkan kebocoran, penyalahgunaan atau pelanggaran privasi individu.	
1. Maklumat Pengenalan Peribadi (PII) merujuk kepada sebarang maklumat yang boleh digunakan untuk mengenal pasti seseorang individu. Ini termasuk, tetapi tidak terhad kepada nama, alamat, nombor telefon, alamat e-mel, nombor pekerja, maklumat kewangan dan data biometrik. 2. MBK hendaklah mengenal pasti dan memenuhi keperluan mengenai pemeliharaan privasi dan perlindungan maklumat peribadi mengikut undang-undang dan peraturan yang terpakai dan keperluan kontrak 3. Pihak pengurusan perlu menggalakkan dasar privasi yang adil dan bertanggungjawab bagi memastikan semua maklumat peribadi digunakan berdasarkan keperluan untuk mengelakkan penyalahgunaan maklumat. 4. Pendedahan maklumat peribadi tentang kakitangan Majlis kepada pihak ketiga tidak sepatutnya berlaku kecuali: a. Dikehendaki oleh undang-undang atau peraturan; b. Dengan persetujuan yang jelas dan nyata daripada kakitangan tersebut; atau c. Setelah menerima persetujuan bertulis daripada pihak ketiga di mana maklumat akan dilindungi dengan tahap keselamatan dan privasi yang mencukupi seperti yang ditentukan oleh Bahagian Undang-Undang serta perjanjian jelas diperoleh daripada pengurusan sumber manusia; dan d. Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian dan pengeluaran yang tidak sah mengikut undang-undang, peraturan, kontrak dan keperluan Majlis.	Warga MBK / Pembekal / Pakar Runding / Pihak yang mengakses dan menggunakan perkhidmatan MBK
5.35 KEBEBASAN SEMAKAN KESELAMATAN MAKLUMAT ***(INDEPENDENT REVIEW OF INFORMATION SECURITY)***	
Memastikan keselamatan maklumat dinilai secara objektif oleh pihak yang tidak terlibat secara langsung dalam operasi harian keselamatan maklumat, bagi mengenal pasti kelemahan, meningkatkan keberkesanan dan memastikan pematuhan terhadap piawaian seperti ISO/IEC 27001	
1. Pendekatan MBK untuk mengurus keselamatan maklumat dan pelaksanaannya termasuk orang, proses dan teknologi hendaklah disemak secara bebas pada selang masa yang dirancang atau apabila perubahan ketara berlaku. 2. Pematuhan pemeriksaan ke atas Polisi Keselamatan Siber, piawaian dan prosedur perlu dilakukan secara tahunan oleh pihak berkecuali atau pihak bebas. Pemeriksaan ini mestilah melibatkan usaha bagi menentukan kawalan yang mencukupi dan dipatuhi;	ICTSO

3. Pengauditan perlu dilaksanakan sekurang-kurangnya sekali setahun terhadap pengoperasian sistem maklumat bagi meminimumkan ancaman dan meningkatkan ketersediaan sistem; dan 4. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.	ICTSO
5.36 PEMATUHAN TERHADAP POLISI, PERATURAN DAN PIAWAIAN KESELAMATAN MAKLUMAT *(COMPLIANCE WITH POLICIES, RULES AND STANDARD FOR INFORMATION SECURITY)* Memastikan semua pengguna, sistem dan proses dalam organisasi mematuhi polisi, peraturan dalaman, dan piawaian yang berkaitan dengan keselamatan maklumat bagi menjaga kerahsiaan, integriti dan ketersediaan data serta aset ICT organisasi.	
1. ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi, piawaian dan keperluan teknikal. Sistem keselamatan maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT. 2. Pematuhan Polisi – Setiap pengguna di MBK hendaklah membaca, memahami dan mematuhi PKS MBK dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT MBK termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. ICTSO/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT, aset maklumat dan aset yang mengandungi maklumat / dokumen MBK selain daripada maksud dan tujuan yang telah ditetapkan oleh pihak pengurusan MBK, adalah merupakan satu penyalahgunaan sumber MBK. 3. Pematuhan dengan Polisi Keselamatan Siber organisasi, peraturan dan piawaian hendaklah sentiasa disemak. 4. Semakan pematuhan boleh dijalankan secara dalaman atau luaran untuk memastikan langkah dan kawalan keselamatan dilaksanakan memenuhi keperluan yang ditetapkan dalam PKS MBK dan undang-undang serta perundangan yang berkenaan.	ICTSO / Pegawai Undang-Undang MBK

5.37 PROSEDUR OPERASI YANG DIDOKUMENKAN *(DOCUMENTED OPERATING PROCEDURE)*	
Memastikan semua aktiviti berkaitan operasi sistem ICT dijalankan secara konsisten, selamat, dan boleh diaudit melalui prosedur bertulis yang jelas dan dikawal selia.	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Semua prosedur keselamatan siber yang diwujudkan, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian serta pemprosesan maklumat, pengendalian serta penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	ICTSO / Pasukan CSIRT MBK / BTM

6.0 KAWALAN SUMBER MANUSIA *(ORGANIZATIONAL CONTROL)*	
KETERANGAN	**PERANAN**
6.1 PEMERIKSAAN *(SCREENING)*	
Memastikan individu yang terlibat secara langsung dalam pengurusan, pembangunan dan penyelenggaraan sistem ICT serta pengendalian maklumat sensitif telah melalui proses saringan latar belakang yang sesuai sebelum dilantik.	
Tapisan keselamatan hendaklah dijalankan terhadap warga Majlis Bandaraya Kuantan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Majlis Bandaraya Kuantan yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga Majlis Bandaraya Kuantan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Majlis Bandaraya Kuantan yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan b. Menjalankan tapisan keselamatan untuk Majlis Bandaraya Kuantan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Majlis Bandaraya Kuantan yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Bahagian Sumber Manusia / Pengarah Jabatan / Ketua Bahagian / Pihak Luar (Pembekal, Pakar Runding dan lain-lain berkenaan)
6.2 TERMA DAN SYARAT PEKERJAAN *(TERMS AND CONDITION EMPLOYMENT)*	
Untuk memastikan semua pegawai dan kakitangan MBK, termasuk kontraktor dan pihak ketiga, memahami dan mematuhi tanggungjawab keselamatan maklumat yang digariskan dalam terma dan syarat pekerjaan mereka.	
Sebagai sebahagian daripada kewajipan kontrak mereka, pekerja, kontraktor dan pengguna pihak ketiga hendaklah bersetuju dan menandatangani terma dan syarat kontrak pekerjaan mereka yang akan menyatakan tanggungjawab mereka dan MBK untuk keselamatan maklumat. Pekerja, kontraktor dan pengguna pihak ketiga hendaklah mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan dan ditandatangani.	Pengarah Jabatan / Ketua Bahagian / Warga MBK / Pihak Luar (Pembekal, Pakar Runding dan lain-lain berkenaan)

6.3 KESEDARAN DAN LATIHAN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY AWARENESS AND TRAINING)*	
Untuk memastikan semua pegawai, kakitangan dan pihak berkepentingan MBK memiliki pengetahuan, kesedaran dan kemahiran yang mencukupi berkaitan keselamatan maklumat bagi melaksanakan tugas dengan selamat dan bertanggungjawab.	
Bagi memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MBK secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa. Perkara-perkara berikut hendaklah dipatuhi: a. Latihan keselamatan dan kempen kesedaran yang berterusan mesti diadakan dengan acara/aktiviti kesedaran berjadual. b. Kekerapan acara/aktiviti hendaklah dinilai secara berkala berdasarkan analisis keperluan latihan yang didokumenkan oleh organisasi, tetapi latihan keselamatan tidak boleh kurang daripada satu sesi latihan setahun untuk semua pekerja. Bukti bahawa latihan telah disediakan mesti dikekalkan. c. Latihan fungsional hendaklah dirancang untuk memastikan kecekapan pekerja. d. Menilai program latihan kesedaran MBK untuk memastikan pekerja dididik tentang amalan terbaik keselamatan, risiko dalam *social engineering* (contoh: *phising email, baiting*) dan peranan mereka dalam mengekalkan persekitaran yang selamat.	ICTSO / Pengurus ICT / Pengarah Jabatan/ Bahagian Sumber Manusia
6.4 PROSES TATATERTIB *(DISCIPLINARY PROCESS)*	
Untuk memastikan tindakan tatatertib diambil secara adil dan berstruktur terhadap mana-mana individu yang melanggar dasar, peraturan atau prosedur keselamatan maklumat MBK.	
1. Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan MBK serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dalam perundangan dan peraturan ditetapkan oleh MBK. 2. Proses tatatertib tidak boleh dimulakan tanpa pengesahan terlebih dahulu bahawa pelanggaran keselamatan telah berlaku. 3. Proses tatatertib formal hendaklah memastikan layanan yang betul dan adil bagi pekerja yang disyaki melakukan pelanggaran keselamatan. 4. MBK hendaklah memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan MBK serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh MBK.	Pengarah Jabatan / Bahagian Sumber Manusia / Bahagian Undang-Undang / Bahagian Integriti

6.5 TANGGUNGJAWAB SELEPAS PENAMATAN ATAU PERTUKARAN PERKHIDMATAN *(Responsibilities after Termination or Change of Employment)*	
Untuk memastikan bahawa semua akses kepada sistem, maklumat, dan aset ICT MBK ditamatkan atau dikemaskini secara selamat apabila berlakunya penamatan atau pertukaran perkhidmatan staf, pembekal, atau kontraktor.	
Warga MBK yang bertukar peranan dan tanggungjawab hendaklah mematuhi perkara-perkara berikut: a. Pertukaran tanggungjawab atau pekerjaan hendaklah diuruskan sebagai penamatan tanggungjawab atau pekerjaan masing-masing, dan tanggungjawab atau pekerjaan baharu itu hendaklah dikawal. b. Memastikan semua aset ICT dikembalikan kepada MBK mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan. c. Hak capaian pengguna hendaklah diselaraskan/dikemaskini selari dengan perubahan pada fungsi kerja mereka (peranan dan tanggungjawab). d. Apabila anggota menamatkan perkhidmatannya dengan MBK, proses/aktiviti *offboarding* dan komunikasi hendaklah dilakukan untuk memastikan perlepasan anggota diuruskan dengan sewajarnya.	Pengarah Jabatan / Ketua Bahagian / Bahagian Sumber Manusia / BTM
6.6 PERJANJIAN KERAHSIAAN ATAU PERJANJIAN TIADA PENDEDAHAN ***(Confidentiality or Non-Disclosure Agreements – NDA)***	
Untuk melindungi maklumat sulit dan data sensitif MBK daripada sebarang pendedahan yang tidak dibenarkan oleh individu dalam atau luar organisasi.	
1. Semua kakitangan MBK bertanggungjawab untuk memastikan bahawa mereka mematuhi dasar yang didokumenkan, prosedur proses dan piawaian yang berkaitan dengan peranan tugas mereka dan melaporkan semua insiden dan peristiwa keselamatan dengan cara yang sesuai. 2. Keperluan untuk perjanjian kerahsiaan atau *non-disclosure* untuk perlindungan maklumat hendaklah dikenal pasti dan disemak secara berkala. 3. Perjanjian mengenai *non-disclosure* maklumat untuk kakitangan dan pihak luar yang mungkin mempunyai capaian kepada maklumat MBK dan capaian kepada kemudahan pemprosesan maklumat perlu diwujudkan bagi memastikan kerahsiaan, integriti dan ketersediaan maklumat terpelihara semasa proses pemindahan maklumat dan perisian di antara Majlis dengan agensi/entiti luar. 4. Keperluan melindungi kerahsiaan meliputi integriti dan kerahsiaan maklumat hendaklah disemak secara berkala dan didokumenkan.	ICTSO / Pengurus ICT / Bahagian Sumber Manusia / Pegawai Undang-Undang

6.7 KERJA JARAK JAUH *(REMOTE WORKING)*	
Untuk memastikan keselamatan maklumat dan aset ICT MBK sentiasa terpelihara semasa pegawai bekerja secara jarak jauh (*remote working*), termasuk bekerja dari rumah, lokasi luar pejabat, atau menggunakan sambungan jauh.	
Perkara yang perlu dipatuhi adalah seperti berikut: 1. Kerja jarak jauh adalah meliputi semua aktiviti capaian di luar MBK. 2. Sebarang aktiviti kerja jarak jauh *(remote working)* hendaklah mendapat kebenaran daripada CDO/ ICTSO/Pengarah Jabatan. 3. Sebarang aktiviti memuat naik atau memuat turun tanpa kebenaran adalah tidak dibenarkan. 4. Aktiviti kerja jarak jauh oleh Pihak Yang Berkepentingan adalah tidak dibenarkan kecuali mendapat kebenaran dari CDO / ICTSO / Pengarah Jabatan dan dipantau oleh pegawai yang bertanggungjawab. 5. Penganjuran mesyuarat boleh dilaksanakan : a. Menggunakan apa-apa aplikasi mesyuarat dalam talian (*online meeting*) yang dibenarkan oleh MBK; b. Pengenalan diri (ID) dan kata laluan mesyuarat hanya boleh diberikan kepada ahli mesyuarat yang terlibat sahaja; c. Ahli mesyuarat hendaklah menggunakan nama penuh dan jabatan sebagai pengesahan kehadiran mesyuarat ; d. Ahli mesyuarat hendaklah menjaga isu kerahsiaan dan tidak dibenarkan merakam dan/atau berkongsi dan/atau menyebarkan rakaman dan/atau apa-apa maklumat tanpa mendapatkan keizinan Pengerusi terlebih dahulu.	ICTSO / Pengarah Jabatan / Warga MBK / Pembekal
6.8 PELAPORAN INSIDEN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY EVENT REPORTING)*	
Untuk memastikan semua kejadian atau insiden keselamatan maklumat dikenal pasti, direkod, dan dilaporkan dengan segera bagi membolehkan tindakan balas yang cepat, tepat dan berkesan.	
1. Semua kakitangan MBK bertanggungjawab untuk memastikan bahawa mereka mematuhi dasar yang didokumenkan, prosedur proses dan piawaian yang berkaitan dengan peranan tugas mereka dan melaporkan semua insiden dan peristiwa keselamatan dengan cara yang sesuai. 2. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan CSIRT MBK dengan kadar segera: a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian. c. Kata laluan atau mekanisme kawalan capaian hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan. d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden	ICTSO / CSIRT MBK / BTM / Warga MBK

yang tidak dijangka. f. Sistem aplikasi kerap kali atau berulang kali mengalami masalah tidak berfungsi dan sebagainya. 3. Prosedur pelaporan insiden keselamatan Siber berdasarkan : a. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; b. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam; dan c. Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan CSIRT MBK; dan d. Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan Dan Pengendalian Insiden Keselamatan Siber Sektor Awam. 4. Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika perlu dikelaskan sebagai insiden keselamatan maklumat.	

7.0 KAWALAN FIZIKAL *(PHYSICAL CONTROL)*	
KETERANGAN	**PERANAN**
7.1 PERIMETER KESELAMATAN FIZIKAL *(PHYSICAL SECURITY PERIMETERS)*	
Memastikan perlindungan menyeluruh terhadap aset, maklumat dan sistem ICT MBK dengan menetapkan sempadan keselamatan fizikal yang jelas dan terkawal bagi menghalang capaian tanpa kebenaran.	
Kawalan perimeter fizikal hendaklah dilaksanakan untuk menghalang capaian tidak sah ke kawasan kritikal seperti bilik *server*, pusat data dan stor peralatan ICT. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b. Menggunakan keselamatan perimeter (halangan seperti dinding, agar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c. Memasang alat penggera atau kamera jika perlu; d. Mengehadkan jalan keluar masuk; e. Mengadakan kaunter kawalan; f. Menyediakan tempat menunggu untuk pelawat-pelawat; g. Mewujudkan perkhidmatan kawalan keselamatan; h. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; i. Melaksanakan keselamatan fizikal di dalam Bahagian Teknologi Maklumat dan Pusat Data/Bilik Server; j. Melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau- bilau dan bencana; k. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan l. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	BTM / Bahagian Pengurusan Bangunan / Bahagian Kawalan Keselamatan
7.2 KEMASUKAN FIZIKAL (*PHYSICAL ENTRY*)	
Mengawal dan menghadkan kemasukan fizikal ke kawasan ICT dan lokasi strategik bagi mengelakkan capaian tanpa kebenaran, kecurian, sabotaj atau kerosakan terhadap aset ICT MBK.	
1. Zon Kawalan Akses a. Zon Terbuka (*Public Zone*): Kawasan awam seperti ruang lobi, kaunter pertanyaan – tidak memerlukan kawalan khas. b. Zon Terhad (*Restricted Zone*): Kawasan pejabat, stor dokumen – hanya kakitangan berkenaan dibenarkan masuk. c. Zon Kritikal (*Critical Zone*): Bilik Server, pusat data, bilik kawalan sistem -dikawal ketat dengan sistem akses khas.	Warga MBK / Pihak Luar

2. Beberapa lapisan kawalan hendaklah dilaksanakan bagi melindungi zon-zon yang disebutkan: a. Kad Akses / Biometrik i. Akses hanya dibenarkan kepada pengguna berdaftar; ii. Pas pekerja hendaklah dipakai sepanjang waktu bertugas; iii. Semua pas pekerja hendaklah diserahkan semula kepada MBK apabila warga MBK berhenti dan bersara atau berpindah keluar; dan iv. Kehilangan pas pekerja mestilah dilaporkan dengan segera kepada pihak pentadbiran Jabatan /Bahagian Pengurusan Bangunan b. Kunci Fizikal (Manual) i. Untuk pintu-pintu yang kurang kritikal, tetapi tetap dikawal. c. CCTV dan Rakaman i. Dipasang di pintu masuk / keluar serta ruang sensitif d. Daftar Masuk Pelawat i. Pihak ketiga / pelawat mendaftar masuk di kaunter daftar/kaunter pertanyaan; dan ii. Setiap pelawat perlu mengimbas *QR Code* dan mengisi log keluar masuk bilik server dan perlu diiringi oleh pegawai pengiring. e. Pas pelawat i. Pihak ketiga perlu mengambil pas pelawat di kaunter pertanyaan /daftar masuk pelawat dan dikembalikan semula selepas tamat urusan; ii. Harus dipakai dengan jelas dan dipakai sepanjang masa semasa berada dalam kawasan MBK; dan iii. Kehilangan pas pelawat mestilah dilaporkan dengan segera kepada pegawai keselamatan MBK f. Log Akses i. Sistem mesti menyimpan log masuk/keluar untuk tujuan audit keselamatan 3. Kemasukan vendor, kontraktor atau pihak luar ke kawasan ICT MBK mestilah berdasarkan permohonan rasmi, kebenaran pengurusan dan pengiring oleh kakitangan bertanggungjawab. Semua peralatan yang dibawa masuk atau keluar hendaklah di rekod dan disahkan. 4. Sebarang kemasukan tanpa kebenaran atau pelanggaran protokol keselamatan fizikal adalah satu kesalahan dan boleh dikenakan tindakan tatatertib, selaras dengan peraturan perkhidmatan dan dasar keselamatan MBK.	Bahagian Pentadbiran / Bahagian Penguatkuasaan dan Kawalan Keselamatan / Bahagian Pengurusan Bangunan / BTM

7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN (*SECURING OFFICES, ROOMS AND FACILITIES*)

Mencegah dari akses fizikal yang tidak sah, kerosakan dan gangguan terhadap maklumat dan aset ICT MBK di pejabat, bilik dan kemudahan.

7.3.1 Keselamatan Pejabat, Bilik dan Kemudahan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Kawasan tempat kerja, bilik mesyuarat, bilik perbincangan, bilik fail, bilik kawalan CCTV, pusat data dan bilik server perlu dihadkan daripada diakses tanpa kebenaran; b. Kawasan tempat bekerja, bilik dan tempat operasi ICT perlu dihadkan daripada akses oleh pihak luar; c. Pegawai pengiring perlu sentiasa berada bersama pihak vendor sekiranya perlu melaksanakan tugas di Pusat Data/Bilik Server; d. Penunjuk ke lokasi bilik operasi (*command centre*) dan tempat larangan tidak harus menonjol dan hanya memberi petunjuk minimum; dan e. Fotografi, video, audio dan peralatan rakaman lain tidak dibenarkan dibawa masuk KECUALI dengan kebenaran CDO, ICTSO atau Pegawai Keselamatan.	Semua pengguna / Warga MBK
7.3.2 Keselamatan Pusat Data	
MBK perlu memastikan semua server di dalam Pusat Data sentiasa selamat daripada pencerobohan atau sebarang ancaman dan membolehkan ia dicapai sepanjang masa. Pusat Data perlu mempunyai kemudahan keselamatan, penyaman udara khas dan kemudahan perlindungan suhu dan kebakaran. a. Pusat Data adalah lokasi yang menjadi tempat pengumpulan atau penyimpanan suatu jenis data. b. Pusat Data menyimpan komputer/server untuk tujuan pengumpulan data dan menukarkannya kepada bentuk yang sesuai bagi kegunaan pengguna atau komputer lain. c. Pusat Data MBK adalah di bawah kelolaan Bahagian Teknologi Maklumat. d. Pusat Data juga seharusnya dilengkapkan dengan ciri-ciri keselamatan lain seperti CCTV dan UPS. Berikut beberapa langkah untuk melindungi server tersebut: a. Memantau dan mengawal keluar masuk pengguna ke pusat data melalui sistem *Security Access Door* dan CCTV; b. Memastikan hanya pegawai-pegawai yang mempunyai kebenaran sahaja yang dibenarkan memasuki Pusat Data; c. Memastikan Pusat Data sentiasa bersih dan peralatan ICT tidak terdedah kepada habuk; d. Memastikan penyaman udara berfungsi dengan baik dan suhunya adalah bersesuaian dengan Pusat Data; e. Memastikan semua peralatan keselamatan, UPS dan penyaman udara mestilah diselenggarakan secara berkala; f. Memastikan Pusat Data juga dilengkapi dengan Sistem Pencegahan dan Penggera Kebakaran yang di selenggara secara berkala; dan g. Memastikan tiada sebarang foto dan video diambil di Pusat Data.	ICTSO / Pegawai Teknologi Maklumat / Penolong Pegawai Teknologi Maklumat
7.3.2 Keselamatan Bilik Server dan Rak Rangkaian	
Bilik Server adalah bilik yang menempatkan server dan peralatan rangkaian serta keselamatan dengan skala dan saiz yang lebih kecil dari Pusat Data. Rak	

rangkaian (mengandungi peralatan rangkaian) sama ada wall standing atau wall mounted (digantung). ICTSO dan Pentadbir Sistem ICT Langkah-langkah keselamatan yang perlu diambil termasuklah: a. Memastikan sistem penyaman udara untuk perlindungan suhu disediakan dalam Bilik Server/Rangkaian berkenaan. Bagi bilik yang memuatkan peralatan rangkaian *wall mounted* perlu mempunyai kitar pengudaraan yang bersesuaian; b. Memastikan sistem pencegahan kebakaran disediakan di bangunan yang mana Bilik Server ditempatkan; c. Memastikan keperluan UPS sekurang-kurangnya mampu melindungi Server dan peralatan rangkaian yang utama; d. Memantau dan mengawal keluar masuk pengguna ke Bilik Server dengan menyediakan Rekod Log Pelawat; e. Memastikan hanya pegawai-pegawai yang mempunyai kebenaran sahaja yang dibenarkan memasuki Bilik Server; f. Memastikan Bilik Server sentiasa bersih dan peralatan ICT tidak terdedah kepada habuk; g. Memastikan penyaman udara mestilah berfungsi dengan baik, di mana suhunya adalah bersesuaian dengan Bilik Server; h. Memastikan semua peralatan di selenggara secara berkala; i. Memastikan rak peralatan server dan rangkaian tidak diletakkan di bawah penyaman udara, kotak suis agihan (DB) elektrik, tingkap atau ruang-ruang terbuka pada persekitaran luar; j. Memastikan tiada sebarang peralatan luar diletakkan di bawah rak *wall mounted* bagi memastikan rak tersebut boleh dicapai pada bila-bila masa; k. Memastikan setiap rak peralatan server dan rangkaian dikunci dan kunci disimpan di tempat yang selamat; dan l. Mempunyai sistem pencegahan kebakaran yang sewajarnya dan bersesuaian.	ICTSO / Pentadbir Sistem ICT (PTM,PPTM)/ BTM / Pengurusan Bangunan
7.4 PEMANTAUAN KESELAMATAN FIZIKAL (*PHYSICAL SECURITY MONITORING*)	
Memastikan kawasan penting MBK sentiasa dipantau, direkodkan dan disemak bagi mencegah sebarang aktiviti yang mencurigakan atau tidak dibenarkan.	
1. Akses tanpa kebenaran ke kawasan fizikal terhad seperti bilik server dan bilik peralatan ICT boleh mengakibatkan kehilangan kerahsiaan, ketersediaan, integriti dan keselamatan aset maklumat. Berikut adalah kawalan yang boleh dilaksanakan: a. Kamera CCTV b. Pengawal keselamatan c. Penggera keselamatan untuk penceroboh d. Alat perisian untuk pengurusan keselamatan fizikal 2. Premis hendaklah dipantau secara berterusan untuk capaian fizikal yang tidak dibenarkan. 3. Semua pelawat, vendor atau kontraktor pihak ketiga tidak dibenarkan untuk mengakses kawasan larangan tanpa pengawasan kakitangan yang	Bahagian Pentadbiran / Bahagian Penguatkuasaan dan Kawalan Keselamatan / Bahagian Pengurusan Bangunan / BTM

dibenarkan. 4. Anggota perkhidmatan sokongan pihak ketiga hendaklah diberi capaian terhad ke kawasan terkawal hanya apabila diperlukan. Akses ini hendaklah mendapat kebenaran dan dipantau. Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan. 5. Log capaian pintu, rakaman CCTV dan status persekitaran hendaklah di selenggara dan disemak secara berkala.	
7.5 PERLINDUNGAN FIZIKAL DAN ANCAMAN PERSEKITARAN *(PROTECTION AGAINST PHYSICAL AND ENVIRONMENTAL THREATS)*	
Melindungi aset MBK daripada ancaman fizikal dan persekitaran yang boleh mengakibatkan kehilangan data, gangguan perkhidmatan atau kerosakan peralatan kritikal.	
1. Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. MBK perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana. 2. Tapak yang dipilih untuk menempat maklumat, sistem dan aplikasi hendaklah dilindungi dengan sewajarnya daripada pencerobohan fizikal, kecurian, kebakaran, banjir, dan bahaya fizikal dan persekitaran yang lain. 3. Sistem dan peralatan MBK yang kritikal hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan dalam utiliti sokongan. 4. Premis MBK termasuklah kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan sistem penggera kebakaran dan gas pemadam kebakaran, sistem amaran pencerobohan fizikal yang boleh memberi amaran secara automatik kepada pihak yang boleh mengambil tindakan segera. 5. Peralatan pemprosesan maklumat serta sokongan utiliti hendaklah di selenggara dan diuji secukupnya untuk memastikan ketersediaan dan integriti yang berterusan. Semua peralatan perlindungan keselamatan hendaklah diperiksa sekurang-kurangnya sekali setahun. 6. Bahan mudah terbakar DILARANG disimpan di dalam kawasan penyimpanan aset ICT dan semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT. 7. Mematuhi peraturan yang telah ditetapkan oleh pihak berkuasa seperti Jabatan Bomba dan Penyelamat, Jabatan Kerja Raya dan sebagainya.	BTM / Bahagian Pentadbiran / Bahagian Pengurusan Bangunan
7.6 BEKERJA DI KAWASAN YANG SELAMAT *(WORKING IN SECURE AREA)*	
Memastikan hanya individu yang diberi kebenaran dibenarkan bekerja di kawasan yang mempunyai peralatan, maklumat atau sistem kritikal serta mengurangkan risiko pendedahan, kerosakan, atau kecurian maklumat.	
Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga MBK yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis MBK termasuklah Pusat Data.	

Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas kawasan tersebut adalah seperti yang berikut: a. Sumber data atau server, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran; b. Akses adalah terhad kepada warga MBK yang telah diberi kuasa sahaja dan dipantau pada setiap masa; *c.* Pemantauan dibuat menggunakan *Closed-Circuit Television* (CCTV) kamera atau lain-lain peralatan yang sesuai; d. Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual; e. Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; f. Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; g. Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam; h. Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan; i. Memperkukuh dinding dan siling; dan j. Menghadkan jalan keluar masuk.	ICTSO / Pegawai Teknologi Maklumat / Penolong Pegawai Teknologi Maklumat
7.7 DASAR MEJA KOSONG DAN SKRIN KOSONG *(CLEAR DESK AND CLEAR SCREEN)*	
Mengurangkan risiko capaian tidak sah, kehilangan dan kerosakan kepada maklumat di meja, skrin dan mana-mana lokasi yang boleh dimasuki sewaktu dan selepas waktu bekerja.	
Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja atau di paparan skrin apabila pengguna tidak berada di tempatnya. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. menggunakan kemudahan *password screen saver*, *logout* apabila meninggalkan komputer atau perisian yang bersesuaian. b. menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci. c. memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimile dan mesin fotostat. d. memastikan media storan mudah alih tidak ditinggalkan di komputer atau di ruang kerja.	Warga MBK

7.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN *(EQUIPMENT SITING AND PROTECTION)*	
Memastikan peralatan ICT MBK ditempatkan secara selamat dan dilindungi daripada akses tanpa kebenaran, kerosakan fizikal, gangguan persekitaran dan ancaman keselamatan lain.	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan atau konfigurasi yang telah ditetapkan; c. Pengguna dilarang sama sekali menambah, menanggalkan atau menggantikan sebarang perkakasan ICT tanpa kebenaran; d. Pengguna tidak dibenarkan memasang sebarang perisian tambahan pada peranti jabatan tanpa kebenaran bertulis daripada Pegawai Aset ICT atau Pengarah Jabatan; e. Pengguna adalah bertanggungjawab atas sebarang kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f. Pengguna mesti memastikan perisian antivirus di komputer mereka sentiasa diaktifkan dan dikemas kini, serta melakukan imbasan ke atas media storan yang digunakan; g. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; h. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau sebarang pengubahsuaian tanpa kebenaran; i. Peralatan kritikal hendaklah disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set* (Gen-Set); j. Semua peralatan ICT hendaklah disimpan atau ditempatkan di lokasi yang teratur, bersih dan mempunyai ciri keselamatan. Peralatan rangkaian seperti *switch, router* dan seumpamanya perlu diletakkan dalam rak khas; k. Peralatan yang digunakan secara berterusan mestilah ditempatkan di kawasan berhawa dingin dan mempunyai sistem pengudaraan (air ventilation) yang bersesuaian; l. Peralatan ICT yang dibawa keluar dari premis MBK mestilah mendapat kelulusan Pegawai Aset ICT / ICTSO serta direkodkan bagi tujuan pemantauan; m. Kehilangan peralatan ICT hendaklah dilaporkan kepada Pegawai Aset ICT dengan kadar segera; n. Pengendalian peralatan ICT hendaklah mematuhi peraturan dan garis panduan semasa yang berkuat kuasa; o. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal tanpa kebenaran Pegawai Aset ICT; p. Sebarang kerosakan peralatan ICT hendaklah dilaporkan melalui Sistem Aduan ICT (Google Workspace) atau Portal Rasmi MBK untuk tindakan pembaikan;	BTM / Warga MBK

q. Pengguna tidak dibenarkan menampal sebarang pelekat pada aset ICT selain pelekat rasmi jabatan bagi menjamin penampilan dan keadaan peralatan; r. Konfigurasi alamat IP tidak boleh diubah daripada tetapan asal yang telah ditentukan oleh pihak ICT; s. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat yang berada di bawah jagaannya dan hendaklah menggunakannya untuk urusan rasmi sahaja; t. Pengguna hendaklah memastikan semua peralatan seperti komputer, pencetak dan pengimbas dimatikan ("OFF") sebelum meninggalkan pejabat; u. Sebarang penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada CSIRT MBK; v. Pengguna hendaklah memastikan palam kuasa (*plug*) dicabut daripada suis utama sekiranya meninggalkan pejabat dalam keadaan cuaca buruk seperti petir atau ribut kilat bagi mengelakkan kerosakan perkakasan; w. Pengguna wajib memastikan penggunaan semua peralatan ICT adalah tertakluk kepada urusan rasmi sahaja dan bukan untuk kegunaan peribadi.	
7.9 KESELAMATAN ASET DI LUAR PREMIS *(SECURITY OF ASSETS OF PREMISES)*	
Memastikan peralatan yang digunakan di luar premis MBK tidak mengalami kehilangan, kerosakan, kompromi keselamatan atau sebarang gangguan yang boleh menjejaskan kelancaran operasi jabatan.	
Peralatan yang dibawa keluar daripada premis MBK adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Peralatan perlu dilindungi dan dikawal sepanjang masa; b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan; c. Sebarang sambungan ke rangkaian dan Internet di tempat awam perlu mengambil kira faktor keselamatan rangkaian terutamanya melibatkan urusan kerja rasmi; d. Peralatan perlu dipastikan tidak digunakan oleh mana-mana pihak ketiga; e. Pergerakan peralatan perlu melalui prosedur yang ditetapkan berserta borang yang berkaitan dan direkodkan bagi tujuan pemantauan; dan f. Sebarang laporan kehilangan peralatan hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa dari semasa ke semasa.	Semua Pengguna / Warga MBK / Pegawai Aset ICT
7.10 MEDIA STORAN *(STORAGE MEDIA)*	
mengawal selia penggunaan dan pengendalian media storan supaya maklumat dan data yang disimpan sentiasa dilindungi daripada kehilangan, kebocoran, kerosakan atau akses tidak dibenarkan.	

1. Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti pemacu USB, cakera keras luaran, cakera optik (CD/DVD), kad memori, *hard disk*, SSD dan storan awan. 2. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. 3. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b. Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja; c. Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak 'dibenarkan, kecurian dan kemusnahan; d. Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; e. Akses dan pergerakan media storan hendaklah direkodkan; f. Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; g. Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan i. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	Warga MBK / BTM / CSIRT MBK
7.11 UTILITI SOKONGAN *(SUPPORTING UTILITIES)*	
memastikan semua utiliti sokongan yang digunakan bagi menyokong operasi ICT di premis MBK berfungsi dengan baik dan tidak menjejaskan kesinambungan operasi ICT, terutamanya semasa berlaku gangguan elektrik atau kecemasan.	
Peralatan ICT perlu dilindungi daripada kegagalan bekalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara perkara yang perlu dipatuhi adalah seperti berikut: a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (generator) boleh digunakan bagi perkhidmatan kritikal seperti di Pusat Data/Bilik Server supaya mendapat bekalan kuasa berterusan;	BTM / Bahagian Pengurusan Bangunan

c. Perancangan untuk keperluan bekalan kuasa untuk semua peralatan hendaklah dibuat sebelum perolehan bagi memastikan bekalan kuasa mencukupi untuk operasi. Kesemua utiliti sokongan perlu diselenggara secara berkala.	
7.12 KESELAMATAN KABEL *(CABLING SECURITY)*	
Melindungi kabel rangkaian dan kuasa daripada akses tanpa kebenaran, kerosakan fizikal dan gangguan perkhidmatan yang boleh menjejaskan keselamatan serta integriti sistem ICT MBK.	
Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut: a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*, dan d. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	BTM / Bahagian Pengurusan Bangunan / Pihak Ketiga (kontraktor ICT berdaftar)
7.13 PENYELENGGARAAN PERKAKASAN *(EQUIPMENT MAINTENANCE)*	
Memastikan semua peralatan ICT MBK diselenggara secara sistematik dan berkala supaya sentiasa berada dalam keadaan optimum, selamat dan mematuhi piawaian keselamatan serta operasi ICT jabatan.	
Peralatan ICT hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti yang berterusan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi yang telah ditetapkan oleh pengeluar; b. Memastikan perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c. Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pegawai Aset ICT	BTM / Warga MBK / Pihak Ketiga (vendor/kontraktor ICT berdaftar)

7.14 PELUPUSAN SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN *(SECURE DISPOSAL OR RE-USE OF EQUIPMENT)*	
Memastikan pelupusan atau penggunaan semula peralatan ICT yang tidak lagi digunakan dilakukan secara selamat, beretika dan mematuhi standard keselamatan bagi mengelakkan kebocoran data atau penyalahgunaan maklumat rasmi jabatan.	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada ianya aset harta modal atau inventori yang dibekalkan oleh MBK dan ditempatkan di MBK. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MBK. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran, b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan, c. Peralatan ICT yang akan dilupuskan sebelum dipinda milik hendaklah dipastikan agar maklumat-maklumat dalam penyimpanan telah dihapuskan dengan cara yang selamat, d. Pegawai aset hendaklah mengenal pasti sama ada peralatan tersebut boleh dilupuskan atau sebaliknya, e. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut, f. Pegawai aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam sistem inventori, g. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa dan h. Semua pegawai dan kakitangan MBK adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut:- i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. ii. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *motherboard* dan sebagainya, iii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di MBK, iv. Memindah keluar dari MBK mana-mana peralatan ICT yang hendak dilupuskan ,dan v. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan aset adalah di bawah tanggungjawab MBK.	Pegawai Aset ICT / BTM

8.0 KAWALAN TEKNOLOGI *(TECHNOLOGICAL CONTROL)*	
KETERANGAN	**PERANAN**
8.1 PERANTI PENGGUNA *(USER END POINT DEVICES)*	
Memastikan semua peranti pengguna (user end point devices) seperti komputer meja, komputer riba, tablet, telefon pintar dan peranti lain yang digunakan untuk mengakses sistem atau maklumat MBK dilindungi daripada ancaman keselamatan siber serta dikendalikan secara bertanggungjawab.	
1. 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: a. Tamatkan sesi aktif apabila selesai tugas; b. Log-off komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan c. Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan. 2. Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek di MBK; b. Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek; c. pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan; dan d. kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam PKS MBK.	Warga MBK / ICTSO / Pegawai Aset ICT / BTM
8.2 HAK AKSES ISTIMEWA *(PRIVILEGED ACCESS RIGHT)*	
Mengawal dan mengurus pemberian hak akses istimewa kepada sistem ICT MBK bagi memastikan keselamatan, integriti, dan kerahsiaan sistem serta data terpelihara daripada penyalahgunaan atau pencerobohan.	
Capaian Sistem Pengoperasian 1. 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. 2. Kemudahan ini juga perlu bagi: a. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan b. Merekodkan capaian yang berjaya dan gagal.	BTM

3. Kaedah-kaedah yang digunakan hendaklah MBK menyokong perkara-perkara berikut: a. Mengesahkan pengguna yang dibenarkan; b. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf administrator ; dan c. Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. 4. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log in* yang terjamin; b. Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; c. Mengehadkan dan mengawal penggunaan program; dan d. Menghadkan tempoh sambungan ke aplikasi yang berisiko tinggi. **Capaian Aplikasi dan Maklumat** 1. Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. 2. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara - perkara berikut hendaklah dipatuhi: a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); c. Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; d. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan e. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	
8.3 SEKATAN AKSES MAKLUMAT *(INFORMATION ACCESSRESTRICTION)*	
Memastikan bahawa capaian kepada maklumat dan sumber ICT MBK dikawal secara ketat dan hanya diberikan kepada individu yang diberi kebenaran, mengikut keperluan tugas dan tahap klasifikasi maklumat.	
Akses kepada maklumat dan aset lain yang berkaitan hendaklah dihadkan menurut dasar kawalan capaian. Pengguna atau sumber hanya akan diberikan capaian sistem yang diperlukan untuk memenuhi peranan dan tanggungjawab mereka sahaja.	Pentadbir Sistem ICT / Warga MBK

8.4 AKSES KEPADA KOD SUMBER *(ACCESS TO SOURCE CODE)*	
Memastikan kod sumber sistem dan aplikasi yang dibangunkan, dihoskan atau digunakan oleh MBK dilindungi daripada akses, pengubahsuaian atau penyebaran tanpa kebenaran yang sah.	
Akses kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Log audit perlu dikekalkan kepada semua capaian kepada kod sumber; b. Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan c. Status hak milik kod sumber bagi semua aplikasi dan perisian hendaklah mengikut kepada perjanjian kontrak dengan pembekal atau pembelian aplikasi dan perisian di pasaran.	BTM ICTSO Pengguna Vendor/Kontraktor
8.5 PENGESAHAN KESELAMATAN *(SECURE AUTHENTICATION)*	
Memastikan setiap pengguna sistem ICT MBK disahkan secara selamat sebelum diberikan akses, serta mengelakkan capaian tidak sah dan penyalahgunaan identiti pengguna.	
1. Teknologi dan prosedur pengesahan selamat (*secure authentication*) hendaklah dilaksanakan berdasarkan sekatan capaian maklumat dan dasar kawalan capaian. 2. Kata laluan hendaklah diuruskan seperti berikut: a. Kata laluan tidak boleh ditulis atau disimpan dalam talian. b. Tidak berkongsi atau mendedahkan kata laluan melalui mana-mana medium, termasuk pentadbir, melainkan untuk tujuan kesinambungan perniagaan yang telah diluluskan oleh pihak pengurusan. c. Tidak menggunakan ciri "*Remember password*" aplikasi. d. Jika akaun atau kata laluan disyaki telah terjejas, laporkan kejadian itu kepada kakitangan masing-masing dan tukar semua kata laluan. 3. Sistem pengurusan kata laluan MBK harus menguatkuasakan pilihan kata laluan berkualiti seperti di bawah: a. Semua kata laluan yang akan digunakan mesti mempunyai sekurang-kurangnya 12 aksara. Pengguna digalakkan menggunakan gabungan huruf, nombor dan simbol. b. Kata laluan yang sukar diteka diperlukan dan tidak boleh berasaskan maklumat peribadi seperti nama keluarga. c. Pengguna digalakkan untuk menukar kata laluan setiap 90 hari. d. Semua kata laluan '*default*' digalakkan untuk ditukarkan semasa proses '*login*' pertama.	BTM / ICTSO Pentadbir Sistem Pengguna Vendor/Kontraktor
8.6 PENGURUSAN KAPASITI *(CAPACITY MANAGEMENT)*	
Memastikan sumber ICT seperti pelayan, rangkaian, storan dan sistem utama mempunyai kapasiti yang mencukupi dan bersesuaian untuk menyokong keperluan operasi semasa dan masa hadapan MBK secara efisien dan selamat.	

1. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. 2. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang. 3. Permintaan kapasiti hendaklah dipantau secara berkala, ditala dan unjuran dibuat mengenai keperluan kapasiti masa hadapan untuk memastikan ketersediaan sistem dan kesinambungan operasi perniagaan.	BTM/ICTSO Pentadbir Sistem Jabatan Pengguna
8.7 PERLINDUNGAN TERHADAP PERISIAN HASAD *(PROTECTION AGAINST MALWARE)*	
Melindungi sistem dan data ICT MBK daripada ancaman perisian hasad (*malware*) seperti virus, trojan, spyware, ransomware, dan lain-lain yang boleh menjejaskan keselamatan, integriti dan ketersediaan maklumat serta sistem.	
1. Aset ICT perlu dilindungi supaya tidak terdedah kepada kerosakan yang disebabkan oleh kod hasad seperti *virus, worm, trojan* dan seumpamanya. Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan *malware* hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. 2. Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan. Sekiranya penggunaan sistem dibenarkan pada aplikasi android seperti telefon, IPAD dan sebagainya perkakasan media yang canggih, peralatan tersebut perlulah mempunyai antivirus untuk melindungi data tersebut daripada digodam atau dicerobohi. 3. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d. Mengemas kini antivirus dengan *signature/pattern* antivirus yang terkini; e. Menyemak kandungan (*patches*) sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi	ICTSO Pentadbir Sistem Pengguna/Warga MBK

program berisiko terhadap perisian; h. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus; dan i. Melaksanakan program kesedaran yang bersesuaian kepada pengguna.	
8.8 PENGURUSAN KELEMAHAN TEKNIKAL *(MANAGEMENT OFTECHNICAL VULNERABILITIES)*	
Memastikan bahawa semua kelemahan teknikal dalam sistem ICT MBK dikenal pasti, dinilai dan ditangani secara sistematik untuk mengurangkan risiko ancaman keselamatan terhadap maklumat dan infrastruktur ICT.	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Melaksanakan ujian penembusan sekurang-kurangnya setahun sekali untuk memperoleh maklumat kelemahan teknikal bagi sistem aplikasi dan operasi sedia ada; b. Memastikan sistem baharu dilaksanakan ujian penembusan untuk memperoleh maklumat kelemahan teknikal sistem aplikasi dan operasi sebelum memulakan pengoperasian; c. Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan d. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan. Pegawai Teknologi Maklumat hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	BTM/Pentadbir Sistem CSIRT MBK Pengguna/Warga MBK
8.9 PENGURUSAN KONFIGURASI *(CONFIGURATION MANAGEMENT)*	
Memastikan semua konfigurasi sistem, perisian, peralatan rangkaian dan aplikasi dikawal dengan teliti bagi menjamin integriti, kestabilan dan keselamatan infrastruktur ICT MBK.	
1. Spesifikasi dan konfigurasi setiap perkakasan dan perisian hendaklah ditentukan, dipantau dan dikawal daripada pengubahsuaian yang tidak dibenarkan. 2. Semua item konfigurasi, termasuk konfigurasi keselamatan perkakasan, perisian, perkhidmatan, rangkaian dan hubungannya hendaklah didokumenkan, di selenggara dan disemak. 3. Item konfigurasi hendaklah diaudit pada selang masa yang tetap untuk mengesan perubahan atau penyelewengan yang tidak dibenarkan daripada garis dasar.	BTM/Pentadbir Sistem Pengarah Jabatan/Ketua Bahagian Pengguna/Warga MBK

8.10 PEMADAMAN MAKLUMAT *(INFORMATION DELETION)*	
Memastikan semua maklumat yang tidak lagi diperlukan dihapuskan dengan selamat bagi mengelakkan kebocoran, penyalahgunaan atau akses tidak sah terhadap data rasmi dan sensitif MBK.	
Maklumat yang disimpan di dalam sistem maklumat, peranti atau di dalam mana-mana media storan lain hendaklah dipadamkan apabila tidak lagi diperlukan. Pengekalan data berbeza mengikut klasifikasi dan jenis maklumat. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	Pegawai Teknologi Maklumat Warga MBK
8.11 DATA MASKING *(DATA MASKING)*	
Melindungi data sensitif dan peribadi dengan menggunakan kaedah *data masking*, agar data tersebut tidak didedahkan secara langsung kepada pengguna atau pihak yang tidak dibenarkan, terutamanya dalam persekitaran ujian, latihan atau pendedahan awam.	
Perkara-perkara yang perlu dipertimbangkan: a. Tahap penyamaran dan/atau penyamaran yang diperlukan, berbanding dengan sifat data. b. Cara data bertopeng sedang diakses. c. Sebarang perjanjian mengikat yang menyekat penggunaan data untuk disembunyikan. d. Mengekalkan data bertopeng berasingan daripada mana-mana jenis data lain, untuk mengelakkan subjek data dikenal pasti dengan mudah. e. Meneliti data yang diterima, dan bagaimana ia telah diberikan kepada mana-mana sumber dalaman atau luaran.	Pentadbir Sistem/Aplikasi Vendor/FTPK Warga MBK
8.12 PENCEGAHAN KEBOCORAN DATA *(DATA LEAKAGE PREVENTION)*	
Melindungi maklumat sulit, sensitif dan data peribadi MBK daripada dipindahkan, diakses, atau didedahkan secara tidak sah kepada pihak ketiga melalui sebarang medium fizikal atau digital.	
Kebocoran data sukar untuk dihapuskan sepenuhnya. Walau bagaimanapun, untuk meminimumkan risiko yang unik untuk operasi, MBK harus: a. Klasifikasikan data selaras dengan piawaian industri yang diiktiraf (PII, data komersial, maklumat produk) untuk menetapkan tahap risiko yang berbeza-beza di seluruh bahagian. b. Memantau dengan teliti saluran data yang diketahui yang banyak digunakan dan terdedah kepada kebocoran (contoh: e-mel,pemindahan fail dalaman dan luaran, peranti USB). c. Hadkan keupayaan pengguna untuk menyalin dan menampal data (jika berkenaan) ke dan dari platform dan sistem tertentu. d. Kebenaran daripada pemilik data sebelum sebarang pemindahandata dilaksanakan. e. Pertimbangkan untuk mengurus atau menghalang pengguna daripada	ICTSO/BTM Pengarah Jabatan Pengguna

mengambil tangkapan skrin atau mengambil gambar monitor yang memaparkan jenis data yang dilindungi. f. Sulitkan sandaran yang mengandungi maklumat sensitif. g. Merangka langkah keselamatan pintu masuk dan langkah pencegahan kebocoran yang melindungi daripada faktor luaranseperti (tetapi tidak terhad kepada) pengintipan industri, sabotaj, gangguan komersial dan/atau kecurian IP. h. Memastikan perisian *operating* sistem dan antivirus sentiasa dikemaskini.	
8.13 SANDARAN MAKLUMAT *(INFORMATION BACKUP)*	
memastikan data dan sistem kritikal MBK dapat dipulihkan sekiranya berlaku kehilangan data, kerosakan sistem, insiden keselamatan siber atau bencana alam.	
1. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan secara berkala atau setiap kali konfigurasi berubah. 2. Salinan pendua maklumat dan perisian sistem hendaklah disediakan dan diuji secara berkala selaras dengan polisi *backup* bagi tujuan kesinambungan operasi pemprosesan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a. Membuat salinan pendua ke atas semua maklumat dan sistem perisian mengikut jadual yang ditetapkan atau apabila berlaku perubahan versi; b. Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; c. Menyimpan salinan pendua di lokasi lain yang selamat; dan d. Menguji sistem pendua bagi memastikan ianya dapat beroperasi dengan normal; e. Menyimpan salinan pendua sekurang-kurangnya lima (5) tahun bagi sistem kritikal dan tiga (3) tahun bagi sistem sokongan; dan f. Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	ICTSO/BTM Pengarah Jabatan Pengguna
8.14 KEMUDAHAN PEMPROSESAN MAKLUMAT YANG BERTINDIH *(REDUNDANCY OF INFORMATION PROCESSING FACILITIES)*	
Memastikan kesinambungan operasi ICT MBK dengan menyediakan kemudahan pemprosesan maklumat gantian (*redundan*) sekiranya berlaku gangguan terhadap kemudahan utama.	
1. Kemudahan pemprosesan maklumat hendaklah dilaksanakan dengan redundansi yang mencukupi untuk memenuhi keperluan ketersediaan. 2. MBK hendaklah menjalankan ujian ke atas sistem maklumat berlebihan untuk memastikan kegagalan daripada satu komponen ke komponen lain berfungsi seperti yang dimaksudkan. 3. Semua sistem aplikasi dan perkakasan yang kritikal hendaklah mempunyai kemudahan *redundancy* dan diuji keberkesanannya mengikut keperluan.	BTM

8.15 LOGGING *(LOGGING)*	
Memastikan semua aktiviti sistem dan pengguna direkodkan *(logging)* bagi tujuan pemantauan, pengauditan, pengesanan insiden keselamatan dan pematuhan kepada dasar keselamatan ICT.	
1. 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. 2. Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan Malaysia dan Kerajaan Negeri Pahang. Log hendaklah dikawal bagi mengekalkan integriti data. Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti yang berikut: a. Fail log sistem pengoperasian; b. Fail log servis (contoh: web); c. Fail log aplikasi (*audit trail*); dan d. Fail log rangkaian (contoh: *firewall*). 3. Pentadbir Sistem mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: a. Sebarang percubaan pencerobohan kepada sistem ICT MBK; b. Serangan kod perosak (malicious code), penolakan perkhidmatan perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); c. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d. Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; e. Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f. Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; g. Aktiviti penyalahgunaan akaun e-mel; dan h. Aktiviti penukaran alamat IP (IP *address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT. 4. Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi	ICTSO Pentadbir Sistem/Aplikasi

susunan dan perubahan dalam sesuatu acara. 5. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: a. Rekod setiap aktiviti transaksi; b. Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang .digunakan; c. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan d. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. 6. Pentadbir Sistem hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan. 7. Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada ICTSO dan CDO.	
8.16 PEMANTAUAN AKTIVITI *(MONITORING ACTIVITIES)*	
Menetapkan garis panduan dalam pemantauan aktiviti ICT bagi menjamin keselamatan maklumat, mengesan insiden keselamatan, serta memastikan pematuhan kepada polisi dan peraturan sedia ada.	
1. Pemantauan kepada rangkaian, sistem dan aplikasi perlu dilaksanakan secara berterusan mengikut tempoh yang bersesuaian. Perkara-perkara yang memerlukan pemantauan termasuklah tetapi tidak terhad kepada: a. Trafik keluar masuk rangkaian, sistem dan aplikasi; b. Capaian kepada sistem, server, perkakasan rangkaian, sistem pemantauan, sistem aplikasi yang kritikal dan lain-lain; c. Tahap pentadbir sistem dan fail konfigurasi rangkaian; d. Log dari peralatan/perisian keselamatan (contoh: Antivirus, IDS, IPS, *firewall* dan lain-lain); e. Log kejadian berkaitan aktiviti sistem dan rangkaian; f. Penggunaan kod yang disahkan tidak disalah guna; dan	ICTSO Pentadbir Sistem Pentadbir Rangkian

g. Penggunaan sumber (contoh: CPU, *hard disks*, *memory* dan *bandwith*). 2. ICTSO mestilah bertanggungjawab menyemak, merekod dan menganalisis perkara-perkara berikut: a. Sebarang percubaan pencerobohan kepada sistem ICT Jabatan/Agensi; b. Aktiviti yang boleh menjadi punca serangan kod hasad *(malicious code)*; c. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d. Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; e. Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f. Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; g. Aktiviti penyalahgunaan akaun e-mel; h. Aktiviti penukaran alamat IP (IP *address*) dan segmen IP selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT; dan i. Sebarang aktiviti yang menyebabkan terdapat keperluan untuk semakan dan forensik ICT dijalankan di bawah arahan CDO dan ICTSO.	
8.17 PENYERAGAMAN WAKTU *(CLOCK SYNCHRONISATION)*	
Memastikan semua sistem, *server*, peralatan rangkaian dan peranti pengguna diselaraskan kepada masa yang tepat dan seragam untuk tujuan keselamatan, integriti log dan penyelarasan operasi.	
Waktu server dan peralatan ICT yang berpusat dan kritikal perlu diselaraskan dengan satu sumber waktu yang piawai menggunakan *Network Time Protocol* (NTP) *Server* atau mana-mana sumber waktu setempat yang mematuhi *Malaysian Standard Time*. Masa yang berkaitan dengan sistem pemprosesan maklumat ICT MBK mestilah diseragamkan mengikut rujukan punca masa yang sama yang digunakan oleh organisasi. Ini untuk memastikan ketepatan masa log yang disimpan serta bertujuan untuk mengawal integriti log tersebut bagi kegunaan masa hadapan.	BTM Pentadbir Sistem ICT

8.18 PENGGUNAAN PROGRAM UITILITI ISTIMEWA *(USE OF PRIVILEGED UTILITY PROGRAMS)*	
Memastikan penggunaan program utiliti tidak mendatangkan mudarat kepada keselamatan maklumat bagi kawalan sistem dan aplikasi.	
Penggunaan program utiliti perlu dikawal dan mematuhi perkara berikut: a. Hanya program atau perisian khas utiliti yang selamat sahaja digunakan. b. Penggunaan program atau perisian khas utiliti yang membebankan kapisiti rangkaian (*bandwith*) perlu dihadkan dan dikawal.	BTM Pentadbir Sistem Pengguna
8.19 PEMASANGAN PERISIAN PADA SISTEM OPERASI *(INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS)*	
Memastikan integriti pada sistem operasi dan mengelakkan eksploitasi kepada kerentanan (*vulnerabilities*) teknikal.	
1. Semua pemasangan perisian pada sistem operasi jabatan hendaklah dikawal dan dipantau dengan rapi untuk mengelakkan risiko keselamatan, ketidakstabilan sistem, dan ketidakpatuhan kepada dasar ICT yang ditetapkan. 2. Hanya perisian yang telah diperakui dan diluluskan oleh Bahagian Teknologi Maklumat (BTM) atau ICTSO sahaja yang dibenarkan untuk dipasang ke atas mana-mana peranti ICT jabatan. 3. Sebarang permohonan pemasangan perisian mesti dikemukakan secara rasmi dan mendapat kelulusan bertulis daripada Pegawai Aset ICT / ICTSO / Pengarah Jabatan sebelum pemasangan dilakukan. 4. Pemasangan perisian hendaklah: a. Melibatkan perisian berlesen dan sah sahaja. b. Dijalankan oleh pegawai teknikal bertauliah atau individu yang diberi kuasa. c. Direkodkan untuk tujuan pemantauan, pengauditan dan keselamatan. d. Melalui proses ujian terlebih dahulu bagi menjamin keserasian dan keselamatan sistem operasi. 5. Pengguna adalah dilarang memasang sebarang perisian tambahan tanpa kebenaran yang sah daripada pihak bertanggungjawab. 6. Kegagalan mematuhi peruntukan ini boleh menyebabkan tindakan tatatertib diambil mengikut peraturan yang berkuat kuasa.	BTM Warga MBK Pembekal/Kontraktor

8.20 KESELAMATAN RANGKAIAN *(NETWORKS SECURITY)*	
Melindungi infrastruktur rangkaian MBK termasuk sistem, peranti dan komunikasi data daripada akses tidak sah, pencerobohan dan serangan siber.	
1. MBK hendaklah memastikan rangkaian teknologi maklumat diurus dan dikawal untuk melindungi maklumat kritikal dalam sistem dan aplikasi daripada ancaman luaran dan dalaman. 2. Rangkaian MBK hendaklah mempunyai kawalan capaian yang ketat, di mana semua pengguna rangkaian tertakluk kepada pengesahan, keizinan, pengesahsahihan, dan penilaian berterusan. 3. Keperluan keselamatan untuk semua perkhidmatan rangkaian hendaklah dikenal pasti tanpa mengira sama ada perkhidmatan ini disediakan secara dalaman atau daripada pihak luar. 4. Reka bentuk rangkaian hendaklah diasingkan mengikut segmen untuk menyediakan keselamatan dan perlindungan. Setiap segmen hendaklah dilindungi mengikut profil risiko dan ancaman masing-masing. 5. Teknik atau teknologi keselamatan perimeter (contoh: DMZ, *firewall*, IPS/IDS) hendaklah digunakan untuk memeriksa dan menyekat trafik rangkaian. 6. Semua sambungan yang mengakses rangkaian hendaklah tertakluk kepada senarai kawal capaian untuk menyekat capaian daripada peranti, pengguna dan sambungan yang tidak dikenali. 7. Peraturan *firewall* hendaklah disemak dan dikemaskini secara berkala untuk memastikan peraturan usang atau salah dialih keluar. Peraturan ini tidak boleh diubah tanpa kebenaran daripada pihak berkuasa. 8. Konfigurasi/tetapan peranti rangkaian dan keselamatan hendaklah disemak secara berkala dan dikemaskini dengan kerap untuk memenuhi keperluan keselamatan dan pematuhan. 9. Perkhidmatan *Network Time Protocol* (NTP) hendaklah dilindungi untuk memastikan penyelarasan sistem jam adalah tepat dan konsisten.	BTM Pentadbir Rangkaian
8.21 KESELAMATAN PERKHIDMATAN RANGKAIAN *(SECURITY OF NETWORK SERVICES)*	
Memastikan keselamatan dalam penggunaan perkhidmatan rangkaian.	
Semua perkhidmatan rangkaian yang disediakan secara *inhouse* atau *outsourced* perlu dikenal pasti mekanisme keselamatan, pengurusan dan tahap perkhidmatan serta perlu dimasukkan dalam perjanjian perkhidmatan rangkaian.	ICTSO Pentadbir Sistem ICT

8.22 PENGASINGAN RANGKAIAN (SEGREGATION OF NETWORKS)	
Memisahkan rangkaian dalam sempadan keselamatan dan mengawal trafik di kalangan rangkaian tersebut berdasarkan keperluan perkhidmatan MBK	
Pengasingan rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian Jabatan/Agensi Negeri seperti berikut: a. Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian MBK. b. Perkhidmatan *Wireless* (WIFI) untuk kegunaan awam hendaklah diasingkan daripada rangkaian dalaman MBK.	Pentadbir Sistem ICT
8.23 PENAPISAN WEB *(WEB FILTERING)*	
Menghalang akses ke laman web berbahaya atau tidak berkaitan tugas rasmi, melindungi sistem ICT daripada ancaman siber, mengawal penggunaan internet dan memastikan pematuhan kepada dasar keselamatan organisasi.	
Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang.	Pentadbir Rangkaian
8.24 PENGGUNAAN KRIPTOGRAFI *(USE OF CRYPTOGRAPHY)*	
Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
Kriptografi merangkumi kaedah-kaedah seperti yang berikut: a. Enkripsi - Sistem aplikasi yang melibatkan maklumat rahsia rasmi hendaklah dibuat dan Semua Pengguna enkripsi (*encryption*); dan b. Tandatangan Digital - Maklumat rahsia rasmi yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media yang mengandungi tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b. Media ini tidak boleh dipindah milik atau dipinjamkan; dan c. Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	ICTSO Pentadbir Rangkaian Warga MBK
8.25 KITAR HAYAT PEMBANGUNAN SELAMAT *(SECURE DEVELOPMENT LIFE CYCLE)*	
Memastikan keselamatan maklumat direka bentuk dan dilaksanakan pada kitar hayat pembangunan perisian dan sistem aplikasi.	
Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Keselamatan persekitaran pembangunan; b. Keselamatan pangkalan data;	ICTSO Pentadbir Sistem ICT Pentadbir Rangkaian

i. Pemantauan Capaian Pangkalan Data di Pelayan Produksi secara berkala; ii. Permohonan Capaian Pangkalan Data di Pelayan Produksi; dan iii. Pewujudan Pangkalan Data Baharu/Peningkatan direkodkan dengan permohonan perlu disertakan dengan dokumen yang berkaitan. c. Keperluan keselamatan dalam fasa reka bentuk; d. Keperluan *check point* keselamatan dalam carta perbatuan projek; e. Keperluan pengetahuan ke atas keselamatan aplikasi; f. Keselamatan dalam kawalan versi; dan g. Bagi pembangunan secara sumber luaran (*outsource*), pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.	
8.26 KEPERLUAN KESELAMATAN APLIKASI *(APPLICATION SECURITY REQUIREMENTS)*	
Memastikan setiap aplikasi yang dibangunkan, digunakan atau diselenggara oleh MBK mematuhi keperluan keselamatan bagi melindungi kerahsiaan, integriti dan ketersediaan data serta sistem ICT.	
1. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi MBK. Contoh perkhidmatan sumber luaran ialah: I. Perisian Sebagai Satu Perkhidmatan; II. Platform Sebagai Satu Perkhidmatan; III. Infrastruktur Sebagai Satu Perkhidmatan; IV. Storan Pengkomputeran Awan; dan V. Pemantauan Keselamatan. b. Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji secara berkala. c. Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (*authentication*); d. Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi; e. Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan f. Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak. 2. Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulang tayang mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi;	ICTSO Pentadbir Sistem ICT

b. Memastikan semua aspek transaksi dipatuhi; c. maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan; d. mengekalkan kerahsiaan maklumat; e. mengekalkan privasi pihak yang terlibat; dan f. protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi. g. Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh Kerajaan	
8.27 SENIBINA SISTEM SELAMAT DAN PRINSIP KEJURUTERAAN *(SECURE SYSTEM ARCHITECTURES AND ENGINEERING PRINCIPLES)*	
Memastikan reka bentuk dan pembangunan sistem ICT MBK dilaksanakan berasaskan prinsip keselamatan yang kukuh, berstruktur dan konsisten dalam semua peringkat pembangunan sistem.	
Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, di selenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V) sektor awam yang terkini. Prinsip keselamatan dalam pembangunan dan sokongan sistem yang berkaitan dengan kejuruteraan sistem perlu dikekalkan dan direkodkan.	BTM Pentadbir Sistem Aplikasi Pembekal
8.28 KESELAMATAN PENGEKODAN *(SECURE CODING)*	
Memastikan semua kod yang dibangunkan bagi sistem aplikasi MBK adalah selamat, bebas daripada kerentanan (*vulnerabilities*) dan mematuhi amalan terbaik pengekodan yang selaras dengan keperluan keselamatan siber.	
Amalan dan prosedur pengekodan yang selamat hendaklah mengambil kira perkara berikut untuk proses pengekodan: a. Prinsip pengekodan perisian yang selamat harus disesuaikan dengan setiap bahasa pengaturcaraan dan teknik yang digunakan. b. Penggunaan teknik dan kaedah pengaturcaraan selamat seperti pembangunan yang hendak dilakukan hendaklah dibuat pengujian dan pengaturcaraan pasangan. c. Penggunaan kaedah pengaturcaraan yang berstruktur. d. Dokumentasi kod yang betul dan penyingkiran kecacatan kod. e. Larangan ke atas penggunaan kaedah pengekodan perisian yang tidak selamat seperti sampel kod yang tidak diluluskan atau kata laluan berkod keras. f. Kod yang digunakan hendaklah sentiasa dikemaskini mengikut keadaan keselamatan semasa.	BTM Penolong Pegawai Teknologi Maklumat Pembangun/Vendor

8.29 UJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN *(SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE)*	
Memastikan sistem dan aplikasi yang dibangunkan oleh MBK telah diuji dari aspek keselamatan secara menyeluruh sebelum diluluskan untuk penggunaan rasmi, bagi mengelakkan risiko kerentanan dan pencerobohan.	
1. Pengujian fungsi keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; b. Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat; dan c. Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan. 2. Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; b. Pengujian penerimaan sistem hendaklah merangkumi Keperluan Keselamatan Sistem Maklumat dan kepatuhan kepada Polisi Pembangunan Selamat; c. Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem diguna pakai; dan d. Pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan (*vulnerability scanner*).	ICTSO BTM Pentadbir Sistem Pembekal/Vendor
8.30 PEMBANGUNAN SUMBER LUAR *(OUTSOURCED DEVELOPMENT)*	
Memastikan bahawa semua aktiviti pembangunan sistem atau aplikasi yang dilaksanakan oleh pihak ketiga (vendor) bagi pihak MBK mematuhi keperluan keselamatan ICT dan melindungi maklumat serta aset MBK daripada ancaman keselamatan.	
Pembangunan aplikasi secara *outsource* perlu diselia dan dipantau oleh pegawai yang dipertanggungjawabkan. Kod sumber (*source code*) bagi aplikasi dan perisian adalah menjadi hak milik MBK. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Perkiraan pelesenan, kod sumber ialah HAK MILIK MAJLIS BANDARAYA KUANTAN dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara *outsource*; b. Bagi semua perkhidmatan sumber luaran, perisian sebagai satu perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori “Pembekal hendaklah membenar Kerajaan hak mencapai kod sumber dan melaksanakan pengolahan risiko"; c. Keperluan kontrak untuk reka bentuk selamat, pengekodan dan	ICTSO Pentadbir Sistem Pembekal/Vendor

pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik; d. Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem; e. Mengguna pakai prinsip dan tatacara *escrow* (sekiranya perlu), dan f. Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian.	
8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, UJIAN DAN PRODUKSI *(SEPARATION OF DEVELOPMENT, TEST AND PRODUCTION ENVIRONMENT)*	
Memastikan persekitaran pembangunan, ujian dan pengeluaran sistem ICT MBK dipisahkan secara fizikal atau logikal bagi mengurangkan risiko gangguan, pencerobohan dan kebocoran data.	
Perkara-perkara yang perlu dipatuhi bagi keperluan pengasingan adalah seperti berikut: a. Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji aplikasi perlu diasingkan dari perkakasan sebenar yang digunakan (*production*) bagi mengurangkan risiko. b. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. c. Kawalan keselamatan pada data yang mengandungi maklumat rahsia rasmi sekiranya digunakan di dalam persekitaran pembangunan. MBK perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: a. Sensitiviti data yang akan diproses, disimpan dan dihantar/diterima dari/ke sistem; b. Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; c. Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem; d. Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; dan e. Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	BTM Pentadbir Sistem Pembekal/Vendor ICTSO
8.32 PENGURUSAN PERUBAHAN *(CHANGE MANAGEMENT)*	
Memastikan semua perubahan terhadap sistem, perisian, perkakasan atau konfigurasi ICT di MBK dikawal, didokumentasi dan diluluskan secara rasmi bagi mengelakkan gangguan operasi, kelemahan keselamatan dan pelanggaran dasar ICT.	
Kawalan Perubahan	
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: a. Pengubahsuaian yang melibatkan peralatan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada Pengarah/Pegawai ICT atau pemilik aset ICT	Semua Pengguna

terlebih dahulu; 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; c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak; dan e. Makluman kepada pengguna perlu dilakukan sekiranya perubahan mengakibatkan gangguan kepada perkhidmatan ICT.	
Prosedur Kawalan Perubahan Sistem	
Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan MBK. Pentadbir Sistem perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal; c. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja; d. Capaian kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja; dan e. Sebarang perubahan perlu direkodkan dan diuji.	Pentadbir Sistem ICT
Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi	
Apabila platform operasi berubah, aplikasi bagi perkhidmatan kritikal hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan maklumat. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform; b. Perubahan platform perlu dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; c. Memastikan perubahan yang sesuai dibuat kepada Pelan Pengurusan Keselamatan Maklumat MBK dan Pelan Pemulihan Bencana (DRP) yang berkaitan.	ICTSO Pentadbir Sistem ICT
Sekatan Ke Atas Perubahan Dalam Pakej Perisian	
Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.	Pentadbir Sistem ICT

8.33 MAKLUMAT UJIAN *(TEST INFORMATION)*	
Memastikan semua perubahan terhadap sistem, perisian, perkakasan atau konfigurasi ICT di MBK dikawal, didokumentasi dan diluluskan secara rasmi bagi mengelakkan gangguan operasi, kelemahan keselamatan dan pelanggaran dasar ICT.	
Semua sistem baru merangkumi sistem yang dikemaskini atau diubahsuai hendaklah memenuhi kriteria yang telah ditetapkan sebelum ianya diterima atau dipersetujui. Ujian fungsi keselamatan harus dijalankan semasa pembangunan sistem. Data ujian mesti dilakukan secara teliti, dikawal dan dilindungi. Data ujian perlu dihapuskan setelah penggunaannya selesai. Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; b. Sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna; c. Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat; dan d. Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan.	Pentadbir Sistem ICT
8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PENGUJIAN AUDIT *(PROTECTION OF INFORMATION SYSTEMS DURING AUDIT TESTING)*	
Memastikan bahawa ujian audit yang dijalankan terhadap sistem maklumat MBK tidak menjejaskan kerahsiaan, integriti dan ketersediaan sistem serta data yang diuji.	
Keperluan dan aktiviti audit yang melibatkan pengujian sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses kelancaran sistem.	ICTSO Juruaudit Dalam Pentadbir Sistem ICT

TAKRIFAN / GLOSARI

NO	PERKATAAN	MAKSUD
1.	**Antivirus**	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, optical disk, flash disk, CDROM untuk sebarang kemungkinan adanya virus.
2.	**Aset ICT**	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
3.	**Aset Alih**	Aset alih bermaksud aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
4.	***Backup* (Sandaran)**	Proses penduaan sesuatu dokumen atau maklumat
5.	**Baki risiko**	Risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan.
6.	***Bandwidth***	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan
7.	**BCP/PKP**	*Business Continuity Planning* Pelan Kesinambungan Perkhidmatan
8.	**BTM**	Bahagian Teknologi Maklumat
9.	**CCTV**	*Closed-Circuit Television System* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
10.	**CIA**	*Confidentiality, Integrity, Availability*
11.	**CDO**	*Chief Digital Officer* Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan maklumat digital bagi menyokong arah tuju sesebuah organisasi.
12.	***Clear Desk dan Clear Screen***	Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
13.	***Denial of service***	Halangan pemberian perkhidmatan
14.	***Defence-in-depth***	Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.
15.	***Dongle***	*Dongle* atau anak kunci ialah ketulan kecil perkakasan komputer yang bersambung kepada komputer.Fungsi biasa *dongle* ialah sebagai pengesahan atur cara komputer.
16.	***Downloading***	Aktiviti muat turun sesuatu perisian.
17.	***Encryption***	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.

18.	***Escrow* (eskrow)**	Sebarang sistem yang membuat salinan kunci penyulitan supaya boleh dicapai oleh individu yang dibenarkan pada bila-bila masa.
19.	***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*).
20.	**CSIRT MBK**	*Computer Security and Incident Response Teams* atau Pasukan Tindak Balas Keselamatan Siber Majlis Bandaraya Kuantan.
21.	***Hard disk***	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
22.	***Hub***	Hab 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.
23.	***ICT***	*Information and Communication Technology* Teknologi Maklumat dan Komunikasi
24.	***ICTSO***	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan siber.
25.	***Internet***	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
26.	***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.
27.	***Intrusion Detection System (IDS)***	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
28.	***Intrusion Prevention System (IPS)***	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Contohnya: Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
29.	**Impak teknikal**	Melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti.
30.	***LAN***	Local Area Network Rangkaian Kawasan Setempat yang menghubungkan komputer.
31.	***Logout***	Log-out komputer Keluar daripada sesuatu sistem atau aplikasi komputer
32.	***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.

33.	***MODEM***	Modulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
34.	***Outsource***	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi- fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
35.	**Perisian Aplikasi**	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti spreadsheet dan word processing ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
36.	***Router***	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
37.	***Screen Saver***	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
38.	***Server***	Pelayan komputer
39.	***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.
40.	***Threat***	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
41.	***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.
42.	***Video Conference***	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
43.	***Video Streaming***	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
44.	***Virus***	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
45.	***Wireless LAN***	Jaringan komputer yang terhubung tanpa melalui kabel.

LAMPIRAN 1 : AKUJANJI KESELAMATAN MAKLUMAT MAJLIS BANDARAYA KUANTAN

AKUJANJI KESELAMATAN MAKLUMAT MAJLIS BANDARAYA KUANTAN

SAYA SEBAGAI KAKITANGAN MAJLIS BANDARAYA KUANTAN, DENGAN SEPENUHNYA DAN RELA HATI BERIKRAR AKAN MENJAGA DAN MELINDUNGI SEGALA MAKLUMAT DI MAJLIS BANDARAYA KUANTAN MELALUI TINDAKAN BERIKUT:

PERTAMA : **MENJAGA KERAHSIAAN DAN KESELAMATAN MAKLUMAT RASMI YANG DIBERIKAN KEPADA SAYA DAN TIDAK AKAN MEMBOCORKAN MAKLUMAT, MENGEDAR ATAU MENGGUNAKAN MAKLUMAT INI UNTUK TUJUAN TIDAK BERKAITAN;**

KEDUA : **MEMASTIKAN MAKLUMAT YANG DISEBARKAN ADALAH TEPAT, BENAR DAN BOLEH DIPERCAYAI DAN MENGHINDARI SEBARANG BENTUK MANIPULASI ATAU PENYUNTINGAN MAKLUMAT YANG BOLEH MENYESATKAN;**

KETIGA : **MEMATUHI SEMUA POLISI DAN PERATURAN ORGANISASI YANG BERKAITAN PENYEBARAN MAKLUMAT RASMI DAN SEMUA TINDAKAN SAYA SELARAS DENGAN UNDANG-UNDANG;**

KEEMPAT : **MEMBERIKAN MAKLUMAT SECARA JUJUR DAN TERBUKA KEPADA MEREKA YANG MEMERLUKANNYA DAN TIDAK AKAN MENYEMBUNYIKAN MAKLUMAT YANG PERLU DIKETAHUI OLEH PIHAK YANG BERKEPENTINGAN;**

KELIMA : **BERJANJI UNTUK MENGAMBIL LANGKAH-LANGKAH KESELAMATAN YANG SESUAI BAGI MELINDUNGI MAKLUMAT DARIPADA ANCAMAN DALAMAN DAN LUARAN;**

KEENAM : **BERTANGGUNGJAWAB DENGAN TINDAKAN PENYEBARAN MAKLUMAT RASMI DAN BERUSAHA UNTUK MEMPERBETULKANNYA JIKA TERDAPAT KESILAPAN;**

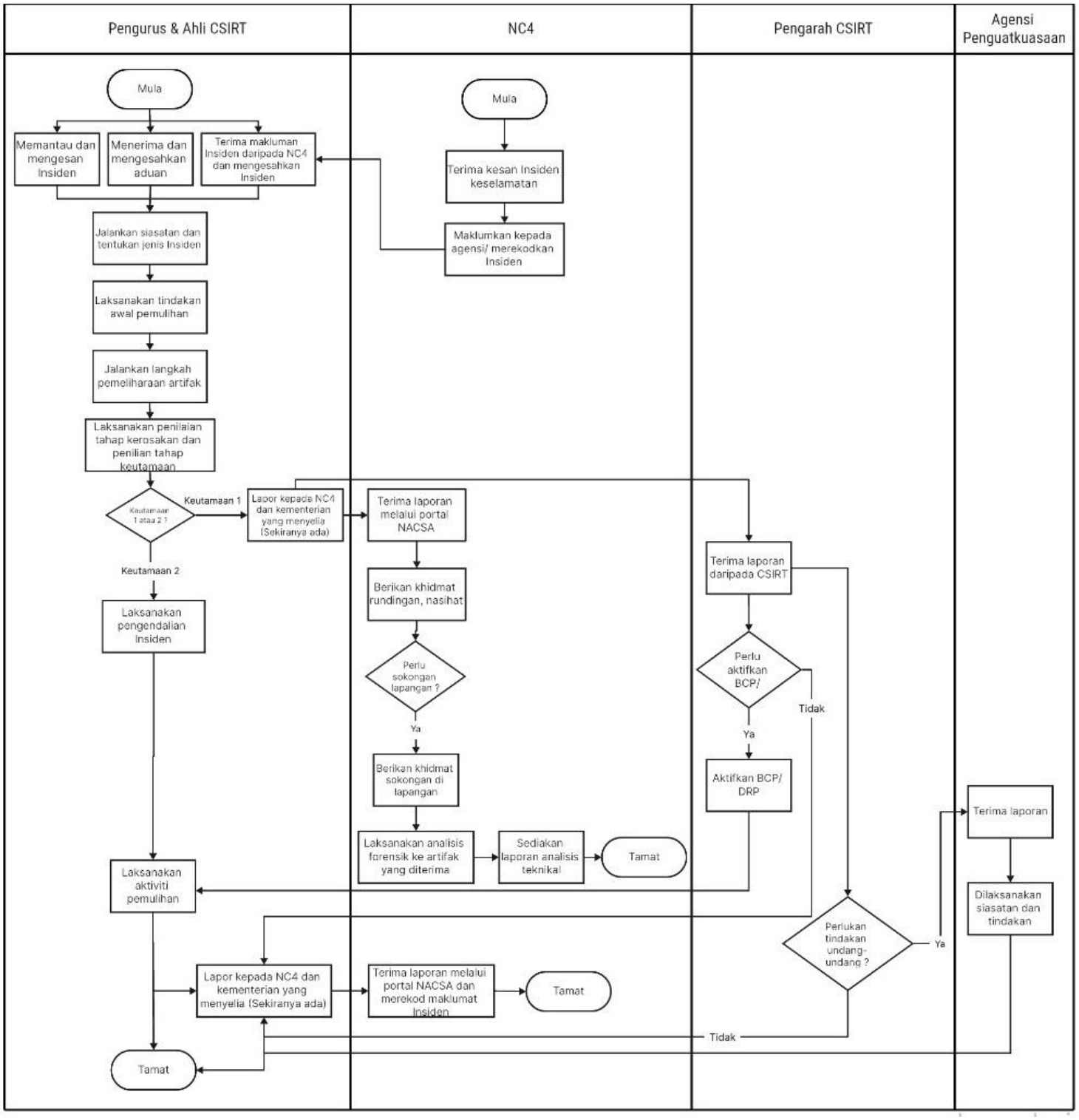
DITANDATANGANI OLEH:

NAMA :
NO. K/P :
JAWATAN :
TARIKH :

DISAKSIKAN OLEH:

DATUK BANDAR
MAJLIS BANDARAYA KUANTAN

LAMPIRAN 2 : PELAPORAN INSIDEN KESELAMATAN ICT MAJLIS BANDARAYA KUANTAN



LAMPIRAN 3 : SURAT PERAKUAN PEMATUHAN AKTA RAHSIA RASMI 1972 DAN POLISI KESELAMATAN SIBER MAJLIS BANDARAYA KUANTAN

PERAKUAN UNTUK DITANDATANGANI OLEH PEGAWAI DAN KAKITANGAN PAKAR RUNDING / KONTRAKTOR / PEMBEKAL BERKENAAN DENGAN AKTA RAHSIA RASMI 1972 DAN AKTA JENAYAH KOMPUTER 1997

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 dan bahawa saya faham sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu benda rahsia adalah menjadi suatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

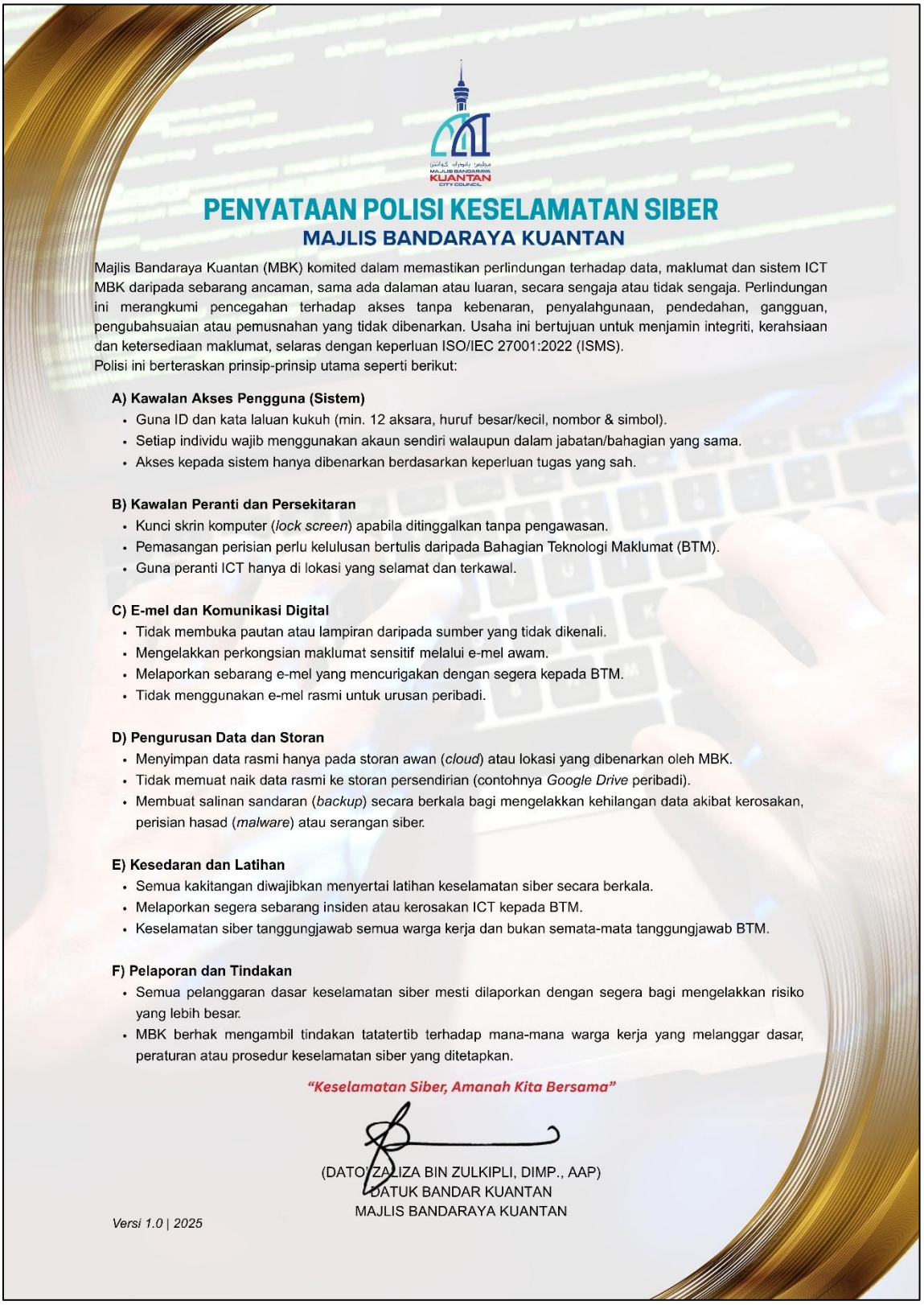
Saya faham bahawa segala maklumat rasmi yang saya perolehi dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan, atau menyampaikan, sama ada secara lisan atau dengan bertulis, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapat kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani suatu akuan selanjutnya bagi maksud ini apabila meninggalkan Perkhidmatan Kerajaan.

Tandatangan : .....
Nama (Huruf Besar) : .....
No. Kad Pengenalan : .....
Jawatan : .....
Jabatan / organisasi : .....
Tarikh : .....
Cop jabatan / Organisasi : .....

Disaksikan oleh : .....
(Tandatangan)

Nama (Huruf Besar) :
No. Kad Pengenalan :
Jawatan :
Jabatan / organisasi :
Tarikh :
Cop jabatan / Organisasi :

LAMPIRAN 4 : PENYATAAN POLISI KESELAMATAN SIBER MAJLIS BANDARAYA KUANTAN



PENYATAAN POLISI KESELAMATAN SIBER
MAJLIS BANDARAYA KUANTAN

Majlis Bandaraya Kuantan (MBK) komited dalam memastikan perlindungan terhadap data, maklumat dan sistem ICT MBK daripada sebarang ancaman, sama ada dalaman atau luaran, secara sengaja atau tidak sengaja. Perlindungan ini merangkumi pencegahan terhadap akses tanpa kebenaran, penyalahgunaan, pendedahan, gangguan, pengubahsuaian atau pemusnahan yang tidak dibenarkan. Usaha ini bertujuan untuk menjamin integriti, kerahsiaan dan ketersediaan maklumat, selaras dengan keperluan ISO/IEC 27001:2022 (ISMS).
Polisi ini berteraskan prinsip-prinsip utama seperti berikut:

A) Kawalan Akses Pengguna (Sistem)
- Guna ID dan kata laluan kukuh (min. 12 aksara, huruf besar/kecil, nombor & simbol).
- Setiap individu wajib menggunakan akaun sendiri walaupun dalam jabatan/bahagian yang sama.
- Akses kepada sistem hanya dibenarkan berdasarkan keperluan tugas yang sah.

B) Kawalan Peranti dan Persekitaran
- Kunci skrin komputer (*lock screen*) apabila ditinggalkan tanpa pengawasan.
- Pemasangan perisian perlu kelulusan bertulis daripada Bahagian Teknologi Maklumat (BTM).
- Guna peranti ICT hanya di lokasi yang selamat dan terkawal.

C) E-mel dan Komunikasi Digital
- Tidak membuka pautan atau lampiran daripada sumber yang tidak dikenali.
- Mengelakkan perkongsian maklumat sensitif melalui e-mel awam.
- Melaporkan sebarang e-mel yang mencurigakan dengan segera kepada BTM.
- Tidak menggunakan e-mel rasmi untuk urusan peribadi.

D) Pengurusan Data dan Storan
- Menyimpan data rasmi hanya pada storan awan (*cloud*) atau lokasi yang dibenarkan oleh MBK.
- Tidak memuat naik data rasmi ke storan persendirian (contohnya *Google Drive* peribadi).
- Membuat salinan sandaran (*backup*) secara berkala bagi mengelakkan kehilangan data akibat kerosakan, perisian hasad (*malware*) atau serangan siber.

E) Kesedaran dan Latihan
- Semua kakitangan diwajibkan menyertai latihan keselamatan siber secara berkala.
- Melaporkan segera sebarang insiden atau kerosakan ICT kepada BTM.
- Keselamatan siber tanggungjawab semua warga kerja dan bukan semata-mata tanggungjawab BTM.

F) Pelaporan dan Tindakan
- Semua pelanggaran dasar keselamatan siber mesti dilaporkan dengan segera bagi mengelakkan risiko yang lebih besar.
- MBK berhak mengambil tindakan tatatertib terhadap mana-mana warga kerja yang melanggar dasar, peraturan atau prosedur keselamatan siber yang ditetapkan.

"Keselamatan Siber, Amanah Kita Bersama"

(DATO' ZALIZA BIN ZULKIPLI, DIMP., AAP)
DATUK BANDAR KUANTAN
MAJLIS BANDARAYA KUANTAN

Versi 1.0 | 2025

LAMPIRAN 5 : RUJUKAN DAN SENARAI PERUNDANGAN DAN PERATURAN

Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di MBK:

1. Arahan Keselamatan
2. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan
3. Pekeliling AM Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)
4. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan
5. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam
6. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam
7. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006
8. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007
9. Surat Arahan Ketua Pengarah MAMPU- Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007
10. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK)
11. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender
12. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan
13. Pekeliling 1PP AM 2 : Tatacara Pengurusan Aset Alih Kerajaan (2.1-2.7)
14. Akta Tandatangan Digital 1997
15. Akta Rahsia Rasmi 1972
16. Akta Jenayah Komputer 1997
17. Akta Hak Cipta (Pindaan) Tahun 1997
18. Akta Komunikasi dan Multimedia 1998
19. Akta Keselamatan Siber 2024 (Akta 854)
20. Perintah-Perintah Am
21. Arahan Perbendaharaan
22. Arahan Teknologi Maklumat 2007
23. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009
24. Surat Arahan Ketua Pengarah MAMPU Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010

25. Surat Arahan YB SUK Pahang : Bil 05 Tahun 2008 : Arahan Keselamatan Penggunaan Komputer Riba Di Jabatan-jabatan Kerajaan Negeri Pahang
26. Surat Arahan YB SUK Pahang (13 Jan 2011) : Larangan Penggunaan Perisian Tidak Berlesen Di Komputer Milik Kerajaan
27. Surat Arahan (28 Mac 2016) : Pelaksanaan Penyelenggaraan Berjadual Bagi Aset ICT Dan Peraturan Kepada Pemilik Aset ICT Pejabat Setiausaha Kerajaan Pahang
28. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) V1.0 MAMPU (April 2016)
29. Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (GCERT) oleh NACSA bertarikh 28 Januari 2019
30. Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022
31. Surat pekeliling am bilangan 2 tahun 2021 Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam
32. Personal Data Protection Act 2010
33. Pekeliling/Arahan/Garis Panduan yang berkuat kuasa dari semasa ke semasa