POLISI KESELAMATAN SIBER
MAJLIS BANDARAYA SHAH ALAM
VERSI 1.0

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
04/04/2024	1.0	Menaiktaraf DKICT kepada Polisi Keselamatan Siber MBSA	04/04/2024
01/08/2024	1.0	Mesyuarat Kajian Semula Pengurusan Tahun 2024 (MKSP 2024)	01/08/2024

JADUAL PINDAAN

TARIKH	VERSI	BUTIRAN PINDAAN
04/04/2024	1.0	*Kemaskini dan menaiktaraf dokumen DKICT MBSA kepada Polisi Keselamatan Siber MBSA (PKS MBSA) berdasarkan ISO/IEC 27001:2022 (ISMS)*

ISI KANDUNGAN

PENGENALAN

Polisi Keselamatan Siber MBSA mengandungi peraturan-peraturan mengenai penggunaan perkakasan dan perisian (aset) teknologi maklumat dan komunikasi (ICT) MBSA. Peraturan-peraturan ini perlu difahami dan dipatuhi oleh semua pengguna di MBSA. Polisi ini juga menerangkan mengenai tanggungjawab dan peranan pengguna dalam melindungi aset ICT MBSA.

OBJEKTIF

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

a) Memastikan kelancaran operasi MBSA bagi mengelak dan meminimumkan kerosakan atau kemusnahan;
b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;
c) Mencegah salah guna atau kecurian aset ICT Kerajaan;
d) Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;
e) Meningkatkan tahap keselamatan ICT kepada para kakitangan, pengguna dan pembekal;
f) Memperkemaskan pengurusan risiko; dan
g) Melindungi aset ICT daripada penyelewengan oleh kakitangan, pengguna dan pembekal.

PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang melibatkan kerosakan atau kejadian yang tidak diingini. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah. Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait

rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:-

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

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

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

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

SKOP

Polisi ini meliputi semua aset ICT MBSA yang terdiri daripada perkakasan, perisian, data / maklumat dan manusia. Polisi Keselamatan Siber MBSA menetapkan keperluan asas berikut:-

a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan

b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Memandangkan sistem ICT sangat kompleks dan terdedah kepada kelemahan, ancaman dan risiko, adalah tidak mudah untuk memenuhi keperluan ini. Sistem ICT dan komponennya yang saling berhubungan dan bergantungan antara satu dengan lain kerap kali mewujudkan pelbagai kelemahan. Sesetengah risiko hanya menjadi kenyataan setelah masa berlalu manakala sesetengahnya timbul apabila berlaku perubahan. Walau bagaimanapun risiko seperti ini hendaklah dikenal pasti dan ditangani sewajarnya.

Bagi menentukan aset ICT ini terjamin keselamatannya sepanjang masa, Polisi Keselamatan Siber MBSA ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, di wujud, di musnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:-

a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan MBSA. Contoh komputer, pelayan (*server*), peralatan komunikasi dan sebagainya;

b) Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data,

perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada MBSA;

c) Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:-

i. Perkhidmatan rangkaian seperti *LAN, WAN* dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses;
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain; dan
iv. Tandatangan digital.

d) Data atau Maklumat

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif MBSA. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod MBSA, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain;

e) Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian MBSA bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

f) Media Storan

Semua media storan dan peralatan yang berkaitan seperti cakera padat, *thumb drive,* pengkomputeran awan dan media storan lain;

g) Media Komunikasi

Semua peralatan berkaitan seperti pelayan (*server*) rangkaian, *gateway*, *bridge*, *router*, peralatan *PABX*, *wireless LAN*, talian *ISDN*, peralatan *video conferencing*, *modem, PCMCIA*, kabel rangkaian, *NIC, switches, hub* dan lain-lain.

h) Dokumentasi

Semua dokumen (prosedur dan manual pengguna) yang berkaitan dengan aset ICT, pemasangan dan pengoperasian peralatan dan perisian, sama ada dalam bentuk elektronik atau bukan elektronik.

i) Premis Komputer Dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara **(a) - (h)** di atas.

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

Polisi Keselamatan Siber MBSA ini juga adalah saling lengkap melengkapi dan perlu dilaksanakan secara konsisten dengan undang-undang dan peraturan yang sedia ada.

Polisi ini adalah terpakai kepada semua pengguna di Majlis Bandaraya Shah Alam termasuk kakitangan, pembekal dan pakar runding yang mencapai, mengurus, menyelenggara, memproses, memuat turun, memuat naik, menyedia, berkongsi, menyimpan dan menggunakan aset ICT Majlis Bandaraya Shah Alam.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Polisi Keselamatan Siber MBSA dan perlu dipatuhi adalah seperti berikut:-

a) Akses Atas Dasar Perlu Mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan akses di bawah prinsip ini adalah berasaskan kepada klasifikasi maklumat dan tapisan keselamatan pengguna seperti berikut *(Sumber: Arahan Keselamatan Bab 4 Keselamatan Rahsia Rasmi, muka surat 31)*:-

i. Klasifikasi Maklumat

Keselamatan ICT Kerajaan hendaklah mematuhi *"Arahan Keselamatan" perenggan 82 - 85, muka surat 32 - 35*, di mana maklumat dikategorikan kepada Rahsia Besar, Rahsia, Sulit dan Terhad. Data, bahan atau maklumat rasmi yang sensitif atau bersifat terperingkat perlu dilindungi dari pendedahan, dimanipulasi atau diubah semasa dalam penghantaran. Penggunaan kod dan tandatangan digital mesti dipertimbangkan bagi melindungi data yang dikirim secara elektronik. Dasar kawalan akses ke atas aplikasi atau sistem juga hendaklah mengikut klasifikasi maklumat yang sama, iaitu sama ada rahsia besar, rahsia, sulit atau terhad; dan

ii. Tapisan Keselamatan Pengguna

Polisi Keselamatan Siber Kerajaan adalah mematuhi prinsip bahawa pengguna boleh diberi kebenaran mengakses kategori maklumat tertentu setelah siasatan latar belakang menunjukkan tiada sebab atau faktor untuk menghalang pengguna daripada berbuat demikian.

b) Hak Akses Minimum

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

c) Kebertanggungjawaban / Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT MBSA hendaklah menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:-

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan kata laluan;
v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.

d) Pengasingan

i. Prinsip pengasingan bermaksud bahawa semua tugas-tugas mewujud, memapar, memadam, mengemaskini, mengubah dan mengesahkan data diasingkan. Ia bertujuan untuk mengelak akses yang tidak dibenarkan dan melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat, dimanipulasi dan seterusnya, mengekalkan kerahsiaan integriti dan kebolehsediaan; dan

ii. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. Ia bertujuan untuk mengasingkan akses kepada domain kedua-dua kumpulan tersebut seperti akses kepada fail data, fail program, kemudahan sistem dan komunikasi, manakala pemisahan antara domain pula adalah untuk mengawal dan mengurus perubahan pada konfigurasi dan keperluan sistem.

Pada tahap minimum, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut:-

i. Persekitaran pembangunan di mana sesuatu aplikasi dalam proses pembangunan;
ii. Persekitaran penerimaan di mana sesuatu aplikasi diuji; dan
iii. Persekitaran sebenar di mana aplikasi sedia untuk beroperasi.

e) Pengauditan

i. Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan (*server*), *router, firewall*, dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau audit trail. Pentingnya audit trail ini menjadi semakin ketara apabila wujud keperluan untuk mengenal pasti punca masalah atau ancaman kepada keselamatan ICT. Oleh itu, rekod audit hendaklah dilindungi dan tersedia untuk penilaian atau tindakan serta merta;

ii. Pengauditan juga perlu dibuat ke atas rekod-rekod manual seperti dokumen operasi, nota serah tugas, kelulusan keluar pejabat, memorandum, borang kebenaran, surat kuasa, senarai inventori dan kemudahan akses log. Ini adalah kerana dalam kes-kes tertentu, dokumen ini diperlukan untuk menyokong *audit trail* sistem komputer; dan

iii. Keseluruhannya, sistem pengauditan ini adalah penting dalam menjamin akauntabiliti. Kebolehan dalam mengakses audit trail bagi setiap peralatan, hanyalah terhad dan terbatas kepada Pentadbir Sistem MBSA sahaja.

Antara lain, sistem ini dapat dirujuk bagi menentukan perkara-perkara berikut:

i. Mengesan pematuhan atau perlanggaran keselamatan;
ii. Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya pelanggaran keselamatan; dan
iii. Menyediakan bahan bukti bagi menentukan sama ada berlakunya pelanggaran keselamatan.

f) Pematuhan

Polisi Keselamatan Siber MBSA hendaklah dibaca, difahami dan dipatuhi. Pematuhan adalah merupakan prinsip penting dalam menghindar dan mengesan sebarang perlanggaran Dasar yang boleh membawa ancaman kepada keselamatan ICT. Pematuhan kepada Polisi Keselamatan Siber MBSA boleh dicapai melalui tindakan berikut:-

i. Mewujudkan proses yang sistematik khususnya dalam menjamin keselamatan ICT untuk memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan;
ii. Merumuskan pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenal pasti;
iii. Melaksanakan program pemantauan keselamatan secara berterusan untuk memastikan standard, prosedur dan garis panduan keselamatan dipatuhi; dan
iv. Menguatkuasakan amalan melaporkan sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan.

g) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Antara lain, pemulihan boleh dilakukan melalui tindakan-tindakan berikut:-

i. Mewujudkan, merumuskan dan menguji Pelan Pemulihan Bencana / kesinambungan perkhidmatan– (*Disaster Recovery Plan / Business Continuity Plan*);
ii. Mengamalkan langkah-langkah membuat salinan data dan lain-lain amalan terbaik dalam penggunaan ICT seperti menghapuskan *virus*, langkah-langkah pencegahan kebakaran, amalan *clear desk* dan *clear screen*; dan
iii. Dalam usaha menaiktaraf aplikasi MBSA, setiap konfigurasi yang diperbaharui hendaklah diuji dahulu di dalam persekitaran penerimaan sebelum digunapakai dalam persekitaran sebenar di mana aplikasi sedia untuk beroperasi. Hal ini demikian adalah untuk mengelakan berlakunya pelanggaran konfigurasi di dalam aplikasi.

h) Saling Bergantung

Langkah-langkah keselamatan ICT yang berkesan memerlukan pematuhan kepada semua prinsip-prinsip di atas. Setiap prinsip adalah saling lengkap melengkapi antara satu dengan lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorak sebanyak mungkin mekanisme keselamatan, dapat menjamin keselamatan yang maksimum. Prinsip saling bergantung meliputi beberapa peringkat di mana di tahap minimum, mengandungi langkah-langkah berikut:-

i. Sambungan kepada Internet – Semua komunikasi antara sistem ICT dengan sistem luar hendaklah melalui mekanisme pusat untuk mengurus, menguatkuasa dan mengawas sebarang bahaya keselamatan. Melalui sistem ini, semua trafik dalaman hendaklah melalui *gateway firewall* yang diurus secara berpusat. Semua trafik dari luar ke dalam hendaklah juga melalui laluan ini atau melalui

kumpulan modem yang dikawal secara berpusat. Dengan itu, penggunaan *modem* dalaman tidak dibenarkan;

ii. *Backbone* Rangkaian – *Backbone* rangkaian akan hanya mengendalikan trafik yang telah dikod untuk meminimumkan intipan;

iii. Rangkaian Jabatan – Semua rangkaian jabatan akan dihubungkan ke *backbone* melalui *firewall* yang mana akan pula mengekod semua trafik di antara rangkaian jabatan dengan rangkaian di peringkat yang seterusnya atau pusat data; dan

iv. Pelayan (*server*) Jabatan – Semua data dan maklumat yang kritikal atau sensitif akan hanya disimpan di pelayan (*server*) jabatan atau di pelayan (*server*) yang diurus secara berpusat. Ini akan meminimumkan pendedahan, pengubahan atau kecurian. Semua data dan maklumat sensitif akan dikodkan.

PENILAIAN RISIKO KESELAMATAN ICT

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

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

Penilaian risiko keselamatan ICT dilaksanakan ke atas sistem maklumat termasuklah aplikasi, perisian, pelayan (*server*), rangkaian dan / atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

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

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

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

PERKARA	PERANAN
ANNEX 5 – KAWALAN ORGANISASI (*ORGANIZATIONAL CONTROLS*)	
5.1 **Polisi Keselamatan Maklumat (*Policies for Information Security*)**	
Objektif: Menerangkan hala tuju, sokongan pengurusan dan peraturan-peraturan terhadap keselamatan maklumat bagi melindungi maklumat dan aset ICT selaras dengan keperluan fungsi-fungsi utama Majlis Bandaraya Shah Alam dan perundangan yang berkaitan.	
5.1.1 **Objektif Dasar**	
Dasar-dasar yang meliputi perkara-perkara berikut telah ditentukan bagi memenuhi objektif Polisi Keselamatan Siber MBSA: a) Pembangunan dan Penyelenggaraan Polisi Keselamatan Siber b) Organisasi Keselamatan c) Pengurusan Aset d) Keselamatan Sumber Manusia e) Keselamatan Fizikal Dan Persekitaran f) Pengurusan Operasi dan Komunikasi g) Kawalan Capaian h) Perolehan, Pembangunan dan Penyelenggaraan Aplikasi i) Pengurusan Pengendalian Insiden Keselamatan j) Pengurusan Kesinambungan Perkhidmatan k) Pematuhan Dasar l) Risikan Ancaman m) Dasar Pencegahan Kebocoran Maklumat	**Semua**

5.1.2	**Pengesahan dan Pelaksanaan Dasar**	
Pengesahan dan pelaksanaan PKS MBSA ini akan dijalankan oleh Datuk Bandar MBSA dibantu oleh ahli dari Mesyuarat Pengurusan yang terdiri daripada Ketua Pegawai Maklumat (CIO), semua Pengarah, Ketua Bahagian, Pengurus Cawangan dan warga MBSA.		**Pengurusan Tertinggi**
5.1.3	**Penyebaran dan Perakuan Dasar**	
Dasar ini disebarkan kepada semua warga MBSA yang terlibat di dalam skop persijilan yang terlibat dengan MBSA iaitu kakitangan, pembekal, pakar runding dan lain-lain. Semua pengguna perlu menandatangani Borang Akuan Akta Rahsia Rasmi 1972 (Akta 88) dan Surat Akuan Pematuhan Polisi Keselamatan Siber MBSA.		**CIO, ICTSO**
5.1.4	**Penyelenggaraan Dasar**	
Dasar ini akan disemak dan dipinda dari semasa ke semasa selaras dengan kemajuan teknologi dan perubahan pada prosedur, perundangan dan perkembangan sosial. Prosedur berhubung penyelenggaraan Polisi Keselamatan Siber MBSA adalah:- a) Mengenal pasti dan menentukan perubahan yang diperlukan; b) Mengemukakan cadangan pindaan untuk mendapatkan persetujuan Mesyuarat Pengurusan; c) Memaklumkan perubahan yang telah dipersetujui oleh mesyuarat kepada semua pengguna; d) Menyemak semula dokumen pada jangka masa yang dirancang mengikut keperluan dan perubahan ketara bagi memastikan dokumen sentiasa relevan dan berkesan.		**ICTSO**
5.1.5	**Pengecualian Dasar**	
Polisi Keselamatan Siber MBSA terpakai kepada semua pengguna ICT MBSA dan tiada pengecualian diberikan.		**Semua**

5.2	**Tanggungjawab dan Peranan dalam Keselamatan Maklumat (*Information Security Roles and Responsibilities*)**

Objektif:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber MBSA.

5.2.1	**Datuk Bandar**	
Peranan dan tanggungjawab Datuk Bandar adalah seperti berikut :- a) Memastikan semua pengguna memahami peruntukan-peruntukan yang telah digariskan di bawah Polisi Keselamatan Siber MBSA; b) Memastikan semua pengguna mematuhi Polisi Keselamatan Siber MBSA; c) Memastikan perlindungan keselamatan adalah mencukupi dari setiap aspek (sumber kewangan, sumber manusia dan perlindungan keselamatan); dan d) Memastikan program/aktiviti kesedaran keselamatan maklumat dan penilaian risiko dilaksanakan.		**Datuk Bandar**

5.2.2	**Ketua Pegawai Maklumat (CIO)**	
Ketua Pegawai Maklumat (CIO) bagi MBSA ialah Timbalan Datuk Bandar MBSA. Peranan dan tanggungjawab CIO adalah seperti berikut:- a) Membantu Datuk Bandar dalam melaksanakan tugas-tugas yang melibatkan keselamatan maklumat; b) Menentukan keperluan keselamatan maklumat; c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan maklumat seperti penyediaan Polisi Keselamatan Siber MBSA serta pengurusan risiko dan pengauditan; d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan maklumat MBSA; dan Menguatkuasakan pelaksanaan Polisi Keselamatan Siber MBSA di semua jabatan/bahagian/pejabat cawangan di MBSA.		**CIO**

5.2.3	Pengarah / Ketua Bahagian	
	Peranan dan tanggungjawab Pengarah / Ketua Bahagian adalah seperti berikut :- a) Memastikan semua pengguna memahami peruntukan-peruntukan yang telah digariskan di bawah Polisi Keselamatan Siber MBSA; b) Memastikan semua pengguna mematuhi Polisi Keselamatan Siber MBSA; c) Memastikan perlindungan keselamatan adalah mencukupi dari setiap aspek (sumber kewangan, sumber manusia dan perlindungan keselamatan); dan Memastikan program/aktiviti kesedaran keselamatan maklumat dan penilaian risiko dilaksanakan.	**Pengarah, Ketua Bahagian**
5.2.4	**Pengarah Digital dan Teknologi Maklumat**	
	Peranan dan tanggungjawab Pengarah Digital dan Teknologi Maklumat adalah seperti berikut:- a) Membantu Datuk Bandar dalam melaksanakan tugas-tugas yang melibatkan keselamatan maklumat; b) Memastikan semua kakitangan, perunding, kontraktor dan pembekal yang terlibat dengan MBSA mematuhi dasar, piawaian dan garis panduan keselamatan maklumat dan seterusnya melaporkan sebarang insiden berkaitan keselamatan maklumat; c) Mengkaji semula aspek-aspek keselamatan fizikal seperti kemudahan *backup* dan persekitaran pejabat yang perlu; d) Melaksanakan keperluan Polisi Keselamatan Siber MBSA dalam operasi semasa seperti berikut:- i. Pelaksanaan sistem atau aplikasi baru sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baru; ii. Pembelian atau peningkatan perisian dan sistem komputer; iii. Perolehan teknologi dan perkhidmatan komunikasi baru;	**Pengarah DTM**

dan iv. Pelantikan pembekal, perunding atau rakan usaha sama. e) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MBSA; f) Membangun, mengkaji semula dan mengemas kini pelan *BCM* keselamatan ICT di MBSA; g) Menentukan kawalan akses pengguna terhadap aset ICT MBSA; h) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CIO; i) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MBSA; dan j) Membangun dan menyelaras pelaksanaan program/aktiviti mengenai keselamatan maklumat.	
5.2.5	**Pegawai Keselamatan ICT (ICTSO)**
Pegawai Keselamatan ICT (ICTSO) bagi MBSA ialah Pegawai Teknologi Maklumat dari Jabatan Digital dan Teknologi Maklumat MBSA. Peranan dan tanggungjawab ICTSO adalah a) Membantu mengurus keseluruhan program-program keselamatan maklumat MBSA; b) Membantu menguatkuasakan pelaksanaan Polisi Keselamatan Siber MBSA; c) Membantu memberi penerangan dan pendedahan berkenaan Polisi Keselamatan Siber MBSA kepada semua pengguna; d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi Keselamatan Siber MBSA; e) Menjalankan pengurusan risiko; f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MBSA berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti *virus* dan memberi khidmat nasihat serta	**ICTSO**

menyediakan langkah-langkah perlindungan yang bersesuaian;

h) Melaporkan insiden keselamatan ICT kepada Pengarah Jabatan Digital dan Teknologi Maklumat MBSA dan memaklumkannya kepada CIO;

i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;

j) Membantu menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT;

k) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan;

l) Memastikan pematuhan Polisi Keselamatan Siber MBSA oleh pihak luaran seperti perunding, kontraktor dan pembekal yang mencapai dan menggunakan aset ICT MBSA untuk tujuan penyelenggaraan, pemasangan, naik taraf dan sebagainya;

m) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan maklumat;

n) Memastikan Polisi Keselamatan Siber MBSA dikemas kini sesuai dengan perubahan teknologi, arahan jabatan dan ancaman-ancaman dari semasa ke semasa; dan

o) Memastikan Pelan Pendigitalan ICT MBSA mengandungi aspek keselamatan maklumat.

5.2.6	**Mesyuarat Pengurusan MBSA**

Mesyuarat Pengurusan bertanggungjawab dalam keselamatan ICT. Keanggotaan adalah seperti berikut:-

Pengerusi : Datuk Bandar MBSA
Ahli : Semua Pengarah Jabatan
Semua Ketua Bahagian
Semua Pengurus Cawangan

Peranan : a) Memperakukan / meluluskan dokumen Polisi Keselamatan Siber MBSA; b) Memantau tahap pematuhan keselamatan ICT; c) Memperakukan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam MBSA yang mematuhi keperluan Polisi Keselamatan Siber MBSA; d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; e) Memastikan Polisi Keselamatan Siber MBSA selaras dengan dasar-dasar ICT kerajaan semasa; f) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; g) Membincangkan tindakan yang melibatkan pelanggaran Polisi Keselamatan Siber MBSA; dan h) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	
5.2.7 **Jawatankuasa Pemandu ICT MBSA (JPICT)**	
Jawatankuasa Pemandu ICT (JPICT) bertanggungjawab dalam keselamatan ICT. Keanggotaan adalah seperti berikut:- Pengerusi : Timbalan Datuk Bandar MBSA atau Timbalan Setiausaha MBSA Urusetia : Jabatan Digital dan Teknologi Maklumat Ahli : Semua Pengarah / Ketua Bahagian / Pengurus Cawangan atau Wakil Peranan : a) Menentukan arah tuju keselamatan Polisi Keselamatan Siber MBSA;	**Ahli Jawatankuasa Pemandu ICT MBSA (JPICT)**

b) Menilai, melulus dan menguatkuasakan pelaksanaan Polisi Keselamatan Siber MBSA; c) Memastikan pengauditan sistem ICT MBSA dilaksanakan; d) Meluluskan program dan aktiviti berkaitan keselamatan maklumat MBSA; e) Memantau ancaman-ancaman utama keselamatan maklumat; f) Melaporkan insiden keselamatan yang telah berlaku dan tindakan yang telah diambil kepada pihak pengurusan MBSA; g) Menyelenggara dokumen Polisi Keselamatan Siber MBSA; h) Memantau tahap pematuhan Polisi Keselamatan Siber MBSA; i) Menilai aspek teknikal keselamatan projek-projek ICT; j) Membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam jabatan yang mematuhi keperluan Polisi Keselamatan Siber MBSA; k) Menyemak semula sistem ICT supaya sentiasa mematuhi keperluan keselamatan dari semasa ke semasa; l) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; dan m) Memastikan Polisi Keselamatan Siber MBSA selaras dengan dasar-dasar ICT Kerajaan semasa.	
5.2.8	**Pengguna**
Peranan dan tanggungjawab pengguna adalah:- a) Membaca, memahami, menandatangani dan mematuhi Polisi Keselamatan Siber MBSA; b) Mengetahui dan memahami implikasi keselamatan maklumat, kesan dari tindakannya dan penglibatan dalam memenuhi keperluan sistem pengurusan keselamatan maklumat; c) Melaksanakan prinsip-prinsip Polisi Keselamatan Siber dan menjaga kerahsiaan maklumat MBSA; d) Melaksanakan langkah-langkah perlindungan seperti berikut :- i. Menghalang pendedahan maklumat kepada pihak yang	**Semua**

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 prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum; viii. Melaporkan sebarang aktiviti yang mengancam keselamatan maklumat kepada ICTSO dengan segera; e) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; f) Menghadiri dan melibatkan diri di dalam program/aktiviti kesedaran mengenai keselamatan maklumat; dan g) Menandatangani *Surat Akuan Pematuhan Polisi Keselamatan Siber MBSA* sebagaimana **Lampiran 1**.	
5.2.9 Pihak Ketiga	
Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain). Perkara yang perlu dipatuhi oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain) bagi memastikan penggunaan maklumat dan kemudahan proses maklumat termasuk yang berikut:- a) Membaca, memahami dan mematuhi Polisi Keselamatan Siber MBSA; b) Mengenal pasti risiko keselamatan maklumat dan kemudahan	**CIO,** **Pengarah DTM,** **ICTSO,** **Pentadbir Sistem Aplikasi,** **Pihak Ketiga**

pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d) Memastikan akses kepada aset ICT MBSA perlu berlandaskan kepada perjanjian kontrak; e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. *Perakuan Akta Rahsia Rasmi 1972;* dan ii. Hak Harta Intelek. f) Pihak ketiga perlu mematuhi dasar keselamatan MBSA serta menandatangani *Non-Disclosure Agreement (NDA)*. g) Menandatangani *Surat Akuan Pematuhan Polisi Keselamatan Siber MBSA* sebagaimana **Lampiran 1**. h) Langkah-langkah harus diambil bagi memastikan segala peraturan atau dasar yang dipatuhi oleh pihak ketiga juga diambil kira bagi seluruh "*supply chain*" (contohnya, sub-kontraktor)	

5.3	**Pengasingan Tugas (*Segregation Of Duties*)**

Objektif:

Menerangkan tugas dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur bagi mengurangkan risiko penipuan, kesilapan serta pemintasan (*bypassing*) kawalan keselamatan maklumat.

5.3.1	**Pentadbir Sistem**

Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut:- a) Memastikan ketepatan dan menyekat kebenaran capaian serta-merta apabila tidak lagi diperlukan atau melanggar Polisi Keselamatan Siber MBSA; b) Melaksanakan prinsip-prinsip Polisi Keselamatan Siber MBSA dan menjaga kerahsiaan maklumat MBSA; c) Menentukan ketepatan dan kesempurnaan kawalan capaian	**Pentadbir Sistem Aplikasi**

pengguna berdasarkan kepada garis panduan keselamatan ICT MBSA; d) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; e) Memantau aktiviti pengguna yang diberi keutamaan capaian yang tinggi dan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi Keselamatan Siber MBSA; f) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi Keselamatan Siber MBSA; g) Memantau aktiviti capaian harian sistem aplikasi pengguna; h) Menjaga kerahsiaan konfigurasi sistem aplikasi dan aset ICT MBSA; i) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; j) Menganalisis dan menyimpan rekod jejak audit; k) Menyediakan laporan mengenai aktiviti capaian secara berkala; dan l) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	
5.3.2	**Pentadbir Rangkaian**
Pentadbir Rangkaian adalah individu yang bertanggungjawab untuk menguruskan dan menyelenggara rangkaian komputer atau sistem komunikasi dalam sebuah organisasi atau syarikat. Skop kerja seorang Pentadbir Rangkaian bergantung kepada saiz dan	**Pentadbir Rangkaian**

kompleksiti rangkaian yang dikendalikan, tetapi secara umumnya, tanggungjawab mereka termasuklah:

a) Pengurusan Rangkaian: Merancang, memasang, mengkonfigurasi, dan menyelenggara rangkaian komputer dan komunikasi. Ini termasuklah penyusunan peralatan keras dan perisian, serta pemasangan dan pengkonfigurasian peranti jaringan seperti router, switch, dan firewall.

b) Pemantauan dan Penyelenggaraan: Memantau prestasi rangkaian secara berkala untuk mengenal pasti masalah atau kelemahan dan menjalankan tindakan penyelenggaraan yang sesuai untuk menyelesaikannya. Ini termasuk juga menyelenggara pelayan, storan data, dan peralatan jaringan lain.

c) Keselamatan Rangkaian: Memastikan keselamatan dan keselamatan data dalam rangkaian dengan melaksanakan langkah-langkah keselamatan seperti penggunaan firewall, pengesahan dua faktor, enkripsi data, dan perlindungan terhadap serangan siber.

d) Penyelenggaraan Perkhidmatan: Menyelenggarakan perkhidmatan rangkaian seperti e-mel, akses internet, intranet, dan aplikasi dalam talian untuk memastikan kebolehpercayaan, kecekapan, dan ketersediaan.

e) Penyelesaian Masalah: Menyiasat dan menyelesaikan masalah rangkaian serta memberikan sokongan teknikal kepada pengguna untuk menyelesaikan masalah yang berkaitan dengan rangkaian.

f) Pemulihan Bencana: Merancang, mengimplementasikan, dan

menguji pelan pemulihan bencana untuk rangkaian bagi memastikan bahawa data dan perkhidmatan penting boleh dipulihkan dengan cepat dalam kejadian bencana atau gangguan serius. g) Pemantauan Trend dan Pertumbuhan: Memantau trend penggunaan rangkaian dan pertumbuhan organisasi untuk menyusun rancangan masa depan rangkaian dan memastikan ia dapat menampung keperluan semasa dan akan datang. h) Kerjasama dengan Pihak Luar: Berkomunikasi dan berinteraksi dengan pembekal perkhidmatan luar, pihak penjual perisian, dan pihak berkuasa berkaitan untuk memastikan kecekapan, keselamatan, dan pematuhan rangkaian. i) Penyelenggaraan Rekod dan Dokumentasi: Menyelenggara rekod dan dokumentasi tentang konfigurasi rangkaian, perubahan yang dilakukan, masalah dan penyelesaiannya, serta pelan pemulihan bencana.	
5.3.3 Pentadbir Laman Web	
Pentadbir Laman Web bertanggungjawab untuk mengurus, menyelenggara, dan memastikan prestasi dan keselamatan laman web organisasi atau syarikat. Skop kerja mereka termasuklah: a) Pembangunan dan Penyelenggaraan Laman Web: Merancang, membangun, dan menyelenggara laman web organisasi mengikut keperluan dan matlamat organisasi. b) Pemantauan dan Pengoptimuman Prestasi: Memantau prestasi laman web secara berkala, termasuk kelajuan muatan, ketersediaan, dan waktu beroperasi, serta menjalankan tindakan pengoptimuman yang diperlukan untuk meningkatkan prestasi. c) Keselamatan Laman Web: Memastikan keselamatan laman web dengan mengambil langkah-langkah seperti memastikan perisian dan plugin sentiasa dikemaskini, mengamalkan praktik	**Pentadbir Laman Web**

keselamatan pengaturcaraan, dan menggunakan SSL untuk melindungi data sensitif. d) Penyelenggaraan Kandungan: Menguruskan dan menyelenggarakan kandungan laman web, termasuk pengemaskinian maklumat, penambahbaikan rekabentuk, dan memastikan konsistensi dan relevansi kandungan. e) Penyelenggaraan Rekod dan Dokumentasi: Menyelenggarakan rekod dan dokumentasi tentang konfigurasi laman web, perubahan yang dilakukan, masalah dan penyelesaiannya, serta pelan pemulihan bencana. f) Pengurusan Domain dan Hosting: Menyelenggara pendaftaran domain, konfigurasi DNS, dan pengurusan pelayan hosting untuk memastikan laman web dapat diakses dengan lancar. g) Integrasi dengan Perkhidmatan Tambahan: Menguruskan integrasi laman web dengan perkhidmatan tambahan seperti e-mel, analitik web, perdagangan elektronik, dan platform media sosial. h) Sokongan Teknikal: Memberikan sokongan teknikal kepada pengguna laman web dalam menyelesaikan masalah atau menawarkan bantuan berkaitan dengan penggunaan dan fungsi laman web. **i)** Kerjasama dengan Pihak Luar: Berkomunikasi dan berinteraksi dengan pembekal perkhidmatan luar, pihak pembangun laman web, dan pihak berkuasa berkaitan untuk memastikan kecekapan, keselamatan, dan pematuhan laman web.	
5.3.4	**Pentadbir Pendaftaran dan Penamatan Pengguna**
Pentadbir Pendaftaran dan Penamatan Pengguna bertanggungjawab untuk menguruskan pendaftaran, penyelenggaraan, dan penamatan akaun pengguna dalam sistem atau platform tertentu. Skop kerja mereka termasuklah: a) Pendaftaran Pengguna: Menguruskan proses pendaftaran pengguna baru dalam sistem atau platform, termasuk pengesahan identiti, pengesahan e-mel, dan penyetujuan akaun. b) Penyelenggaraan Pengguna: Memastikan maklumat pengguna diselenggarakan dengan betul dalam pangkalan data, termasuk butiran peribadi, keahlian, dan kebenaran akses. c) Penyelenggaraan Kategori atau Peranan Pengguna: Menguruskan peranan dan kebenaran pengguna dalam sistem, termasuk pengesahan dan pengurusan akses bagi pengguna	**Pentadbir Pendaftaran dan Penamatan Pengguna**

berdasarkan peranan atau kategori tertentu. d) Pengurusan Kebenaran Akses: Menyelenggara dan mengawal kebenaran akses pengguna kepada fungsi, kandungan, atau data dalam sistem, memastikan hanya pengguna yang dibenarkan memiliki akses yang sesuai. e) Penamatan Akaun Pengguna: Menguruskan proses penamatan akaun pengguna, termasuk penamatan secara manual oleh permintaan pengguna atau sebagai tindak balas terhadap pelanggaran terma dan syarat. f) Penyelenggaraan Rekod dan Audit: Menyelenggara rekod dan audit mengenai aktiviti pendaftaran dan penamatan pengguna, termasuk log masuk, perubahan kebenaran akses, dan penamatan akaun. g) Sokongan kepada Pengguna: Memberikan sokongan teknikal kepada pengguna yang mengalami masalah dalam proses pendaftaran, penamatan akaun, atau pengurusan kebenaran akses. h) Keselamatan dan Kepatuhan: Memastikan proses pendaftaran dan penamatan akaun mematuhi dasar keselamatan dan privasi data, serta peraturan undang-undang berkaitan seperti PDPA. i) Pemantauan Trend dan Analisis: Memantau trend penggunaan sistem, termasuk pertumbuhan pengguna, corak pendaftaran, dan keperluan penamatan, untuk membantu dalam perancangan strategik dan pematuhan. j) Pelaporan dan Analisis: Menyediakan laporan dan analisis berkaitan dengan aktiviti pendaftaran dan penamatan pengguna kepada pihak pengurusan atau pemegang kepentingan yang berkaitan.	
5.3.5	**Pentadbir E-mel**
Pentadbir E-mel, bertanggungjawab untuk mengurus, menyelenggara, dan memastikan keselamatan serta prestasi sistem e-mel organisasi atau syarikat. Skop kerja mereka termasuklah: a) Pengurusan Akaun Pengguna: Membuat, menyelenggara, dan memadam akaun pengguna dalam sistem e-mel, termasuk menetapkan peranan dan kebenaran akses yang sesuai. b) Konfigurasi dan Pemantauan Sistem: Memasang, mengkonfigurasi, dan menyelenggara perisian dan pelayan e-mel, serta memantau prestasi sistem untuk memastikan ketersediaan dan kecekapan.	**Pentadbir E-mel**

c) Keselamatan Sistem: Memastikan keselamatan sistem e-mel dengan melaksanakan langkah-langkah seperti pengesahan dua faktor, enkripsi data, dan perlindungan terhadap serangan siber seperti *phishing* atau *spam*. d) Pengurusan Antara Muka: Menguruskan antara muka pengguna bagi memudahkan pengguna dalam mengakses dan menggunakan sistem e-mel, termasuk penyesuaian konfigurasi, templat, dan tetingkap. e) Penyelenggaraan Kandungan: Menyelenggara kandungan dalam e-mel organisasi, termasuk penyampaian pengumuman, bulletin, atau pemberitahuan kepada pengguna yang berkaitan. f) Pemantauan Keselamatan dan Pematuhan: Memantau aktiviti e-mel untuk mengesan ancaman keselamatan dan melaksanakan tindakan yang diperlukan untuk mematuhi peraturan undang-undang dan dasar organisasi. g) Integrasi dengan Aplikasi Tambahan: Menguruskan integrasi sistem e-mel dengan aplikasi tambahan seperti kalender, aplikasi chat, dan sistem pengurusan tugas bagi meningkatkan produktiviti dan kerjasama. h) Sokongan Teknikal: Memberikan sokongan teknikal kepada pengguna dalam menyelesaikan masalah atau menawarkan bantuan berkaitan dengan penggunaan dan fungsi sistem e-mel. i) Kerjasama dengan Pihak Luar: Berkomunikasi dan berinteraksi dengan pembekal perkhidmatan e-mel luar, pihak keselamatan siber, dan pihak berkuasa berkaitan untuk memastikan kecekapan, keselamatan, dan pematuhan sistem e-mel.	
5.3.6	**Pentadbir *Active Directory* (AD)**
Pentadbir *Active Directory* (AD) bertanggungjawab untuk menguruskan, menyelenggara, dan memastikan keselamatan sistem direktori dalam persekitaran *Microsoft Windows Active Directory*. Berikut adalah beberapa aspek utama dari skop kerja mereka: a) Pengurusan Objek: Mencipta, mengubahsuai, dan memadam objek-objek seperti pengguna, kumpulan, komputer, dan peranti lain dalam struktur direktori *Active Directory*. b) Pengurusan Pengguna dan Kumpulan: Menguruskan pendaftaran pengguna, menyelenggara keahlian kumpulan, serta mengawal akses dan kebenaran pengguna terhadap sumber daya dalam domain.	**Pentadbir *Active Directory* (AD)**

c) Pengurusan Sekuriti: Menetapkan dasar keselamatan dan polisi akses yang sesuai untuk memastikan keamanan data dan sistem. Ini melibatkan pelaksanaan kawalan akses, pemeriksaan dan pengesahan, serta menguruskan kumpulan dasar keselamatan. d) Konfigurasi dan Penyelenggaraan: Menyelenggara dan mengkonfigurasi peranti seperti pelayan domain, pelayan pendaftaran, dan pengawal domain untuk memastikan operasi yang lancar dan kebolehpercayaan. e) Pemantauan dan Pengoptimuman: Memantau prestasi dan kebolehpercayaan sistem AD, mengenal pasti dan menyelesaikan masalah, serta menjalankan tindakan pengoptimuman untuk meningkatkan kecekapan dan keselamatan. f) Pengurusan Polisi: Menguruskan polisi kumpulan dan objek, termasuk kawalan pihak berkuasa, gubahan, dan sekatan polisi untuk mematuhi keperluan keselamatan dan peraturan organisasi. g) Integrasi dan Kerjasama: Berinteraksi dengan aplikasi dan perkhidmatan lain dalam persekitaran IT organisasi untuk menyediakan integrasi yang lancar dan kerjasama antara sistem. h) Sokongan Teknikal: Menyediakan sokongan teknikal kepada pengguna dalam menyelesaikan masalah berkaitan dengan akses dan penggunaan sistem AD. i) Pematuhan dan Audit: Memantau pematuhan terhadap dasar keselamatan dan peraturan, serta menjalankan audit berkala untuk memastikan kepatuhan dan keselamatan yang diperlukan.	
5.3.7	**Pentadbir Pangkalan Data**
Pentadbir Pangkalan Data (DBA) bertanggungjawab untuk merancang, mengurus, menyelenggara, dan memastikan prestasi, keselamatan, dan ketersediaan pangkalan data organisasi. Berikut adalah beberapa aspek utama dari skop kerja mereka: a) Pengurusan Pangkalan Data: Membuat, mengkonfigurasi, dan mengurus pangkalan data organisasi, termasuk pemilihan dan pemasangan perisian pangkalan data serta penentuan struktur pangkalan data yang sesuai. b) Pemantauan dan Pengoptimuman Prestasi: Memantau prestasi pangkalan data secara berkala untuk mengenal pasti masalah atau kelemahan, serta menjalankan tindakan pengoptimuman	**Pentadbir Pangkalan Data**

untuk meningkatkan kecekapan dan respons sistem. c) Penyelenggaraan Keselamatan: Melaksanakan langkah-langkah keselamatan pangkalan data, termasuk pengurusan kebenaran akses, pengenkripsian data sensitif, dan pelaksanaan tindakan keamanan untuk melindungi daripada serangan siber dan kehilangan data. d) Penyelenggaraan Ketersediaan: Memastikan ketersediaan pangkalan data dengan merancang dan menguruskan cadangan data yang berkala, serta merancang dan menguji pelan pemulihan bencana untuk pemulihan data yang cepat dan berkesan. e) Penyelenggaraan Data: Menjaga integriti data dengan memastikan pengurusan data yang betul, termasuk penyelarasan, penyingkiran data yang tidak diperlukan, dan pemeliharaan data berkala. f) Pemantauan Keselamatan dan Pematuhan: Memantau pematuhan terhadap dasar keselamatan dan peraturan, serta menjalankan audit berkala untuk memastikan kepatuhan dan keselamatan yang diperlukan. g) Pengurusan Kapasiti: Mengurus kapasiti dan pertumbuhan pangkalan data dengan merancang, memantau, dan menguruskan penggunaan sumber daya untuk memastikan prestasi yang optimum dan mengelakkan kejatuhan sistem. h) Pengurusan Penyelarasan: Memastikan pangkalan data selaras dengan keperluan aplikasi dan pengguna dengan memantau dan mengurus skema pangkalan data, indeks, dan statistik. i) Pengurusan Reproduksi: Menyediakan dan menyelenggara replikasi data bagi memastikan ketersediaan data yang berkualiti dan kebolehpercayaan operasi. j) Sokongan Teknikal: Memberikan sokongan teknikal kepada pengguna dan pasukan pembangunan dalam menyelesaikan masalah atau memberikan panduan dalam penggunaan dan pemeliharaan pangkalan data.	
5.3.8	**Pentadbir Backup Data**
Pentadbir Backup Data bertanggungjawab untuk merancang, mengkonfigurasi, mengurus, dan memantau operasi serta pemulihan data dalam sistem backup organisasi. Berikut adalah beberapa aspek utama dari skop kerja mereka: a) Merancang Sistem Backup: Menganalisis keperluan penyimpanan dan keperluan pemulihan data organisasi untuk	**Pentadbir Backup Data**

merancang sistem backup yang sesuai, termasuk pemilihan teknologi, peranti, dan perisian yang sesuai. b) Pemasangan dan Konfigurasi: Memasang, mengkonfigurasi, dan menguruskan perisian dan peranti backup, termasuk pelayan backup, storan jaringan (NAS), penyimpanan teras, dan peranti penyimpanan lainnya. c) Penjadualan Backup: Menjadualkan operasi backup secara berkala untuk memastikan data organisasi disalin dengan teratur dan dikekalkan dalam keadaan yang konsisten. d) Pemantauan Operasi Backup: Memantau operasi backup secara berkala untuk memastikan bahawa proses berjalan seperti yang dijangka, serta mengenal pasti dan menyelesaikan masalah yang timbul dengan segera. e) Pengurusan Kapasiti: Mengurus kapasiti penyimpanan backup dan merancang strategi retensi data untuk memastikan penyimpanan yang efisien dan pemulihan data yang sesuai dengan peraturan dan keperluan organisasi. f) Pemulihan Data: Menyelenggarakan ujian pemulihan dan menjalankan operasi pemulihan data apabila diperlukan, termasuk pemulihan sebahagian atau sepenuhnya data dari salinan backup. g) 7. Keselamatan Data: Memastikan keselamatan data dalam salinan backup dengan melaksanakan kawalan akses, enkripsi data, dan langkah-langkah keselamatan lainnya untuk melindungi daripada kehilangan atau akses tidak dibenarkan. h) Pemeliharaan Sistem: Melaksanakan tugas pemeliharaan berkala pada sistem backup, termasuk pembaharuan perisian, ujian prestasi, dan penggantian peranti yang rosak atau usang. i) Sokongan Teknikal: Memberikan sokongan teknikal kepada pengguna atau pasukan IT dalam menyelesaikan masalah yang berkaitan dengan operasi backup dan pemulihan data. j) Pelaporan dan Audit: Menyediakan laporan berkala tentang operasi backup dan pemulihan data, serta menjalankan audit berkala untuk memastikan pematuhan terhadap dasar keselamatan dan peraturan.	

5.4	Tanggungjawab Pengurusan (*Management Responsibilities*)

Objektif:

Untuk memastikan pengurusan memahami peranan mereka dalam keselamatan maklumat dan melaksanakan tindakan yang bertujuan untuk memastikan semua kakitangan menyedari dan memenuhi tanggungjawab keselamatan maklumat mereka.

5.4.1	Pengurusan Tertinggi MBSA	
	Peranan dan tanggungjawab Pengurusan Tertinggi adalah bagi memastikan perkara-perkara berikut :- a) Memastikan semua pengguna memahami Polisi Keselamatan Siber MBSA yang telah ditetapkan; b) Memastikan semua pengguna mematuhi Polisi Keselamatan Siber MBSA; c) Perlindungan keselamatan adalah mencukupi dari setiap aspek (sumber kewangan, sumber manusia dan perlindungan keselamatan); dan d) Program keselamatan maklumat dan penilaian risiko dilaksanakan.	**Pengurusan Tertinggi MBSA**

5.5	Hubungan Dengan Pihak Berkuasa (*Contact With Authorities*)

Objektif:

Memastikan komunikasi berkenaan keselamatan maklumat dilaksanakan melalui saluran yang sesuai antara organisasi dan pihak berkuasa, badan perundangan undang-undang dan lain-lain pihak berkuasa yang berkaitan.

	Menyediakan Pelan Kesinambungan Perkhidmatan (PKP) bagi memastikan kelancaran proses jika berlaku sebarang insiden. PKP pihak berkuasa (undang-undang, polis, penguatkuasa, jabatan bomba dan penyelamat, perubatan, pihak berkuasa utiliti) dihubungi sekiranya insiden yang berkaitan berlaku. Maklumat perhubungan dengan pihak berkuasa harus disimpan dan dikemas kini selalu untuk persediaan pada setiap masa. a) Senarai Maklumat Perhubungan seperti nama, e-mel, no telefon, alamat dan boleh dirujuk melalui Laman Web MBSA	**UPB, Jabatan Penguatkuasaan MBSA**

b) Pelan Kesinambungan Perkhidmatan (PKP) c) Manual Pengurusan Bantuan Bencana	

5.6	Hubungan Dengan Pihak Berkepentingan (Contact With Special Interest Groups)

Objektif:

Memastikan komunikasi berkaitan dengan kumpulan khusus/ pakar dapat dilaksanakan bagi meningkatkan kemahiran dan pengetahuan berkenaan keselamatan maklumat.

Proses yang sesuai harus ditentukan untuk memastikan maklumat mengenai ancaman yang muncul, teknologi keselamatan baru, amalan keselamatan terbaik, amaran awal dan nasihat mengenai kelemahan yang baru ditemui diterima.	**Jabatan Khidmat Pengurusan, JDTM**

5.7	Perisikan Ancaman (*Threat Intelligence*)

Objektif:

Memastikan kesedaran berkenaan ancaman keselamatan maklumat organisasi dapat dilaksanakan supaya tindakan mitigasi yang bersesuaian dapat diambil.

Perisikan Ancaman (TI), juga dikenali sebagai perisikan ancaman siber iaitu amalan mengumpul, menganalisis dan menyebarkan maklumat yang dikumpul daripada sumber dalaman dan luaran tentang potensi risiko yang ditimbulkan kepada keselamatan maklumat MBSA. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Sistem pemantauan keselamatan (*Security Monitoring System*) digunakan bagi mengesan aktiviti yang mencurigakan atau ancaman perisikan yang mungkin terjadi di dalam rangkaian atau sistem. Contoh: Laporan pemantauan keselamatan rangkaian, Laporan *Security Posture Assessment* (SPA) dan	**Pengarah JKP, Pengarah DTM, ICTSO**

perisian Antivirus; b) Memasang *Firewall* bagi mengawal lalu lintas jaringan rangkaian daripada aktiviti yang mencurigakan. Contoh: *Check Point Firewall*, *Web Application Firewall* (WAF); c) Melaporkan hasil analisa Perisikan Ancaman (*Threat Intelligent*) kepada Jawatankuasa Pemandu ICT (JPICT).	

5.8	**Keselamatan Maklumat di dalam Pengurusan Projek (Information Security in Project Management)**

Objektif:
Memastikan risiko keselamatan maklumat telah ditentukan sepanjang projek berlangsung.

Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Elemen keselamatan maklumat perlu diterapkan bagi setiap pengurusan projek di MBSA; 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 mengenai pasti kawalan-kawalan yang diperlukan; dan d) Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam Polisi Keselamatan Siber MBSA (PKS MBSA).	**Semua**

5.9	**Maklumat Inventori & Aset-aset Lain Yang Berkaitan (*Inventory Information & Other Related Assets*)**	
Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MBSA.		
Memastikan semua aset MBSA diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut:- a) Memastikan semua aset MBSA dikenal pasti dan maklumat aset direkod dalam Daftar Aset Alih & Daftar Aset Tidak Ketara dan sentiasa dikemaskini; b) Memastikan semua aset MBSA mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c) Memastikan semua pengguna mengesahkan penempatan aset yang ditempatkan di MBSA; d) Mengenalpasti peraturan bagi pengendalian aset MBSA serta di dokumen dan dilaksanakan; e) Setiap pengguna adalah bertanggungjawab ke atas semua aset MBSA di bawah kawalannya; dan f) Sebarang perlanggaran hendaklah dilaporkan kepada Pegawai Aset / ICTSO.		**Pegawai Aset Jabatan, Pemegang Inventori dan Semua**

5.10	**Kebenaran Penggunaan Maklumat dan Aset Berkaitan (*Acceptable Use of Information and Other Associated Assets*)**	
Objektif: Memastikan maklumat dan aset lain yang berkaitan dilindungi, digunakan dan dikendalikan dengan sewajarnya.		
Perkara yang perlu dipatuhi adalah seperti berikut:- a) Aset yang dipinjam oleh pengguna perlulah direkodkan di dalam Sistem Pengurusan Aset dan maklumat pinjaman direkodkan serta dikemaskini; b) Peminjam aset bertanggungjawab dan memastikan aset		**Pegawai Aset, Semua**

yang dipinjam tidak boleh diberi kepada individu atau peminjam lain; c) Pegawai Aset perlu mengenalpasti aset yang dimohon untuk peminjaman dan memastikan aset tersebut berada dalam keadaan baik; d) Pegawai Aset harus bertanggungjawab dan memastikan aset yang dipinjamkan adalah aset yang berdaftar; e) Peminjam aset harus mematuhi tatacara pinjaman dan prosedur yang telah ditetapkan oleh pihak majlis	

5.11	Pemulangan Aset (*Returns of Assets*)
Objektif: Melindungi aset organisasi sebagai sebahagian daripada proses menukar atau menamatkan pekerjaan, kontrak atau perjanjian.	
Pemulangan bagi peminjaman aset MBSA perlulah mematuhi proses yang berikut: a) Peminjam hendaklah memulangkan semula aset MBSA sebaik sahaja selesai penggunaan atau tempoh perkhidmatan / peminjaman telah tamat. b) Pegawai Aset perlu memastikan pemulangan aset yang dipinjam berada dalam keadaan yang baik dan jumlah aksesori yang dibekalkan mencukupi. c) Pegawai aset harus memastikan merekodkan pemulangan aset di dalam Sistem Pengurusan Aset dan dikemaskini oleh peminjam. d) Jika terdapat kerosakan, peminjam perlu mengisi borang aduan kerosakan bagi membolehkan proses pembaikan dilakukan. e) Peminjam aset bertanggungjawab sepenuhnya ke atas perkakasan / peralatan / aset dan menggunakan aset tersebut bagi tujuan kerja-kerja rasmi majlis.	**Pegawai Aset,** **Semua**

5.12	Pengelasan Dan Pengendalian Maklumat (*Classification of Information*)	
Objektif: Memastikan pengenalan dan pemahaman tentang keperluan perlindungan maklumat selaras dengan kepentingannya kepada organisasi.		
5.12.1	**Pengelasan Maklumat**	
Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian. Maklumat hendaklah dikelaskan dan mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Garis Panduan Keselamatan Perlindungan Tahun 2023 iaitu:- a) Rahsia Besar; b) Rahsia; c) Sulit; atau d) Terhad		**JKP**

5.12.2	Pengendalian Maklumat	
Langkah-langkah keselamatan perlu diambil kira ketika mengendalikan maklumat seperti mengumpul, menghantar, menyimpan, memproses, menyampai, menukar dan ketika memusnahkan maklumat. Langkah-langkah keselamatan yang perlu diambil adalah:- a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) Menjaga kerahsiaan kata laluan; d) *Disable "remember me password"*; e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;		**Semua**

f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum; h) Menentukan maklumat sedia untuk digunakan; i) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih dan / atau ganti rugi sekiranya perisian tersebut mengandungi program berbahaya; j) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan k) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan *virus*.	

5.13	**Pelabelan Maklumat (*Labeling Information*)**
Objektif: Memudahkan komunikasi klasifikasi maklumat dan menyokong automasi maklumat pemprosesan dan pengurusan.	
Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan dokumen Garis Panduan Keselamatan Perlindungan Tahun 2023.	**Semua**

5.14	**Pemindahan Maklumat (*Information Transfer*)**
Objektif: Mengekalkan keselamatan maklumat yang dipindahkan di dalam organisasi dan juga pihak ketiga.	

5.14.1	Pemindahan Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis platform komunikasi; b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara MBSA dengan agensi luar; c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MBSA; dan d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.		**Semua**
5.14.2	**Penggunaan E-mel**	
Penggunaan e-mel dipantau secara berterusan oleh Pentadbir e-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam *Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003* bertajuk *"Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"* dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut:- a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh MBSA sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b) Dalam keadaan yang memudaratkan perkhidmatan MBSA, penggunaan selain e-mel MBSA adalah dibenarkan oleh CIO; c) Sebarang penghantaran dokumen rasmi hendaklah menggunakan e-mel rasmi MBSA; d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-		**Semua**

mel rasmi dan pastikan alamat e-mel penerima adalah betul; e) Semua e-mel hendaklah melalui proses *scanning* untuk memastikan e-mel yang diterima atau dihantar tidak mempunyai *virus*. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi dua puluh lima megabait (25MB) semasa penghantaran. Kaedah pemampatan (*zip file*) untuk mengurangkan saiz adalah disarankan; f) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan serta mengemaskini *mailbox* masing-masing; g) Pengguna dinasihatkan tidak membuka e-mel yang mencurigakan; h) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; i) Maklumat lanjut mengenai keselamatan e-mel bolehlah merujuk kepada *Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003* bertajuk *"Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan";* j) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; k) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; l) Menghadkan jenis dan saiz fail lampiran bagi tujuan mengelakkan jangkitan *virus* dan serangan e-mel *bombing*; m) Penggunaan e-mel MBSA bagi tujuan peribadi adalah tidak dibenarkan;	

n) Pentadbir e-mel perlu menetapkan had minimum kuota *mailbox*; o) Pembersihan e-mel hendaklah dibuat sekiranya *mailbox* didapati tidak aktif selama tiga (3) bulan atau melebihi kuota dan had masa yang ditetapkan; p) Fungsi *Auto-Reply* adalah tidak dibenarkan kecuali pengguna yang bercuti atau bertugas di luar pejabat iaitu dengan menggunakan mesej *Out-of-Office*; q) Pengguna adalah dilarang sama sekali menggunakan alamat e-mel rasmi MBSA bagi pendaftaran dalam mana-mana web / kumpulan / forum yang tidak berkaitan dengan urusan kerja rasmi; dan r) Bahagian Sumber Manusia MBSA perlu memaklumkan sebarang status pengguna (bertukar jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke MBSA) di bahagian masing-masing bagi tujuan pengemaskinian e-mel yang terlibat. Pelanggaran kepada mana-mana peraturan boleh menyebabkan penggantungan akaun pengguna atau mana-mana tindakan tatatertib yang bersesuaian.	
5.14.3 **Business Information System**	
Maklumat yang terlibat dalam perkongsian data di antara sistem aplikasi perlu dilindungi. Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Maklumat yang terlibat perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b) Maklumat yang terlibat dalam transaksi dalam talian (*online*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan c) Integriti maklumat yang disediakan untuk sistem yang	**Semua**

boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	

5.15	**Kawalan Capaian (*Access Control*)**

Objektif:

Kawalan capaian bertujuan mengawal capaian pengguna ke atas aset ICT MBSA dan melindunginya dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.

5.15.1	**Keperluan Kawalan Capaian**	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, di dokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kawalan capaian ke atas Aset MBSA mengikut keperluan keselamatan dan peranan pengguna; b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d) Kawalan ke atas kemudahan pemprosesan maklumat.		**ICTSO dan Pentadbir Sistem Aplikasi**

5.15.1.1	**Capaian Rangkaian**	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:- a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MBSA, rangkaian agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati		**ICTSO dan Pentadbir Sistem Aplikasi**

kesesuaian penggunaannya; dan c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; d) Permohonan capaian perlu mendapat kebenaran pentadbir sistem dengan mendaftarkan keterangan komputer.	
5.15.1.2 **Capaian Internet**	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Penggunaan Internet di MBSA hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, *virus* dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MBSA; b) Kaedah *Content Filtering* boleh digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; c) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; d) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pengarah/ pegawai yang diberi kuasa; f) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; g) Bahan rasmi hendaklah disemak dan mendapat pengesahan	**Pengarah DTM, Ketua Seksyen Operasi & Teknikal**

daripada Pengarah / Ketua Bahagian / Pengurus Pejabat Cawangan sebelum dimuat naik ke Internet;

h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;

i) Sebarang bahan yang dimuat turun dari sumber internet/ laman web yang selamat hendaklah digunakan untuk tujuan yang dibenarkan oleh MBSA;

j) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan;

k) Penggunaan *modem* atau '*broadband'* untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan

l) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:-

   i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan

   ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.

Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada *Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003* bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*".

5.15.2	Kawalan Capaian Sistem Pengoperasian	
5.15.2.1	Capaian Sistem Pengoperasian	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi:- a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; b) Merekodkan capaian yang berjaya dan gagal; dan Kaedah-kaedah yang digunakan hendaklah MBSA menyokong perkara-perkara berikut:- a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan; b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user/super admin*; c) Menjana amaran (*alert*) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem; d) Menyediakan tempoh penggunaan mengikut kesesuaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; b) Mewujudkan satu pengenalan diri (*ID*) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; c) Menghadkan dan mengawal penggunaan program; dan d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	**ICTSO,** **Pentadbir Sistem Aplikasi**	

5.15.2.2	Kad Akses	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Penggunaan kad akses kakitangan dan tempat letak kenderaan hendaklah digunakan bagi memasuki premis Majlis; b) Kad akses hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c) Pelawat perlu mendapatkan kad pelawat di lobi untuk akses ke premis majlis yang telah ditetapkan; d) Sebarang kehilangan, kerosakan dan sekatan perlu dimaklumkan kepada JDTM MBSA.		**ICTSO,** **Pentadbir Sistem Aplikasi**

5.15.3	Kawalan Capaian Aplikasi Dan Maklumat	
5.15.3.1	**Capaian Maklumat Dan Sistem Aplikasi**	
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi:- 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) Menghadkan capaian sistem dan aplikasi kepada minima tiga (3) kali percubaan adalah disyorkan. Sekiranya gagal, akaun atau kata laluan pengguna boleh 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.		**ICTSO,** **Pentadbir Sistem Aplikasi**

5.16	Pengurusan Identiti (*Identity Management*)

Objektif:

Membenarkan pengenalan unik individu dan sistem yang mengakses maklumat organisasi dan aset lain yang berkaitan dan untuk membolehkan penyerahan hak akses yang sesuai.

5.16.1	Akaun Pengguna	

Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, Pentadbir Sistem perlu mengambil langkah-langkah berikut:-

Semua

a) Pengguna perlu mendaftar akaun pengguna menggunakan Borang Permohonan Pendaftaran dan Penamatan Akaun Pengguna;

b) Akaun yang diperuntukkan oleh MBSA sahaja boleh digunakan;

c) Akaun pengguna (*user id*) hendaklah unik;

d) Pemilik akaun pengguna bukanlah hak mutlak pengguna dan ia tertakluk kepada peraturan MBSA. Akaun pengguna boleh disekat dan ditarik balik jika pengguna melanggar peraturan yang ditetapkan;

e) Tidak semua pengguna boleh mencapai semua peringkat maklumat. Terdapat peringkat-peringkat di dalam capaian maklumat dan ditentukan oleh Pentadbir Sistem Aplikasi. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;

f) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan

g) Akaun pengguna boleh dibekukan dan ditamatkan atas sebab-sebab berikut:-

   i. Cuti belajar;

   ii. Bertukar bidang tugas kerja;

iii. Bertukar ke agensi lain; iv. Bersara; v. Digantung perkhidmatan ; atau vi. Ditamatkan perkhidmatan	

5.17	**Maklumat Pengesahan (*Authentication Information*)**	
Objektif: Memastikan pengesahan entiti yang betul dan mencegah kegagalan proses pengesahan.		
5.17.1	**Pengurusan Kata Laluan**	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MBSA seperti berikut:- a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau di kompromi; c) Panjang kata laluan disyorkan sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus; d) Kata laluan hendaklah dihafal dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e) Kata laluan *windows* dan *screen saver* disyorkan diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g) Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas kata laluan di set semula; h) Kata laluan hendaklah berlainan daripada pengenalan identiti	**Pentadbir Sistem Aplikasi dan Semua**	

pengguna; i) Disyorkan had masa pengesahan selama dua (2) minit / mengikut kesesuaian sistem dan selepas had itu, sesi ditamatkan; j) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan k) Mengelakkan penggunaan semula kata laluan yang baru digunakan. l) Kata laluan asal (*default password*) mesti ditukarkan selepas pemasangan perisian atau perkakasan baru.	

5.18	**Hak Capaian (*Access Rights*)**	
Objektif: Memastikan capaian kepada maklumat dan aset lain yang berkaitan ditakrifkan dan dibenarkan mengikut keperluan organisasi.		
5.18.1	**Semakan Hak Capaian Pengguna**	
Penetapan dan penggunaan ke atas hak capaian perlu disemak dari masa ke semasa, diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas bagi memastikan tiada berlaku penyalahgunaan hak capaian.		**Pentadbir Sistem Aplikasi**
5.18.2	**Pembatalan atau Kemaskini Hak Capaian**	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Hak capaian pengguna untuk kemudahan pemprosesan data dan maklumat hendaklah dibatalkan selepas tamat perkhidmatan, kontrak atau perjanjian; dan b) Kemaskini hak capaian pengguna perlulah dilakukan apabila berlaku perubahan dalaman atau perubahan bidang tugas.		**Pentadbir Sistem Aplikasi**

5.19	**Keselamatan Maklumat Dalam Hubungan Dengan Pembekal (*Information Security In Supplier Relationship*)**

Objektif:

Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dengan pembekal.

Keperluan keselamatan maklumat hendaklah dipersetujui dan di dokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset Majlis Bandaraya Shah Alam. Perkara-perkara lain yang perlu diteliti dan dipatuhi seperti berikut: a) Mengenai pasti dan mendokumenkan jenis pembekal mengikut kategori; b) Proses kitaran hayat (*life cycle*) 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) Pelan kontigensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat; g) Melaksanakan program kesedaran terhadap Polisi Keselamatan Siber MBSA kepada pembekal; h) Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber MBSA (Lampiran 3); dan i) Pembekal perlu mematuhi arahan keselamatan yang berkuatkuasa.	**JKP, JDTM,** **Pemilik Projek**

5.20	**Perjanjian Keselamatan Maklumat Dengan Pembekal (*Addressing Information Security Within Supplier Agreements*)**

Objektif:

Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dengan pembekal.

Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi. Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak Majlis Bandaraya Shah Alam selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa. Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Majlis Bandaraya Shah Alam mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara-perkara lain yang perlu diteliti dan dipatuhi seperti berikut: a. Memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan; b. Syarikat pembekal yang mempunyai persijilan 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; f. Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti berikut: i. Badan penilai pihak ketiga adalah bebas dan berintegriti; ii. Badan penilai pihak ketiga adalah kompeten; iii. Kriteria penilaian; iv. Parameter pengujian; dan Andaian yang dibuat berkaitan dengan skop penilaian. g. Pembekal hendaklah bersetuju dan mematuhi semua	**Jabatan Perundangan,** **Pengarah DTM,** **ICTSO,** **Pembekal**

keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan Majlis Bandaraya Shah Alam ; dan h. Pembekal hendaklah mematuhi klasifikasikan maklumat yang telah ditetapkan oleh Majlis Bandaraya Shah Alam.	

5.21	**Pengurusan Keselamatan Maklumat Dalam Rantaian Komunikasi Maklumat ICT (*Managing Information Security In The Information And Communication Technology (ICT) Supply Chain*)**

Objektif:

Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dengan pembekal.

Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara lain yang perlu diteliti dan dipatuhi seperti berikut: a. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b. Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan c. Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	**Pengarah DTM, Pemilik Projek,** **Pembekal**

5.22	**Pemantauan, Semakan Dan Perubahan Pengurusan Perkhidmatan Pembekal (*Monitoring, Review And Change Management Of Supplier Services*)**

Objektif:

Untuk mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal.

1. Majlis Bandaraya Shah Alam hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara lain yang perlu diteliti dan dipatuhi seperti 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 c) Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian. 2. Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan, dengan mengambil kira kepentingan maklumat, sistem dan proses perniagaan yang terlibat dan penilaian semula risiko. Perkara-perkara lain yang perlu diteliti dan dipatuhi seperti berikut: a. Perubahan dalam perjanjian dengan pembekal; b. Perubahan yang dilakukan oleh Majlis Bandaraya Shah Alam bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan c. Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan subkontraktor.	**Pengarah JDTM, Pemilik Projek, Pembekal**

5.23	**Keselamatan Maklumat Bagi Penggunaan Perkhidmatan Awan (*Information Security for Use of Cloud Services*)**

Objektif:

Untuk menentukan dan mengurus keselamatan maklumat untuk penggunaan perkhidmatan awan.

Perkhidmatan awan adalah penting untuk memastikan bahawa organisasi memilih penyedia perkhidmatan awan yang mempunyai tahap keselamatan yang tinggi.

Walaupun terdapat kepentingan dalam menggunakan perkhidmatan awan; konfigurasi yang salah dan pengurusan yang tidak cekap boleh menjejaskan perkhidmatan. Kawalan ini menekankan penyediaan proses yang lebih baik untuk mengakses, menggunakan, mengekalkan, dan keluar dari infrastruktur awan.

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) Melakukan penilaian risiko untuk mengenal pasti potensi ancaman dan kerentanan yang berkaitan dengan penggunaan perkhidmatan awan. Ini memungkinkan anda untuk mengenal pasti tahap risiko dan mengambil tindakan untuk mengurangkan risiko tersebut. c) Memilih penyedia perkhidmatan awan yang mematuhi piawaian keselamatan maklumat dan memiliki rekod prestasi yang baik dalam bidang keselamatan dan privasi data. d) Membuat perjanjian perkhidmatan dengan penyedia perkhidmatan awan yang merangkumi butiran keselamatan maklumat, seperti tahap layanan, perlindungan data, pematuhan piawaian, pemisahan data, pemulihan bencana, dan peraturan pematuhan.	**ICTSO, Pentadbir Rangkaian**

e) Melakukan audit keselamatan secara berkala ke atas penyedia perkhidmatan awan untuk memastikan pematuhan mereka terhadap perjanjian perkhidmatan dan piawaian keselamatan maklumat. f) Memastikan bahawa penyedia perkhidmatan awan mempunyai perancangan pemulihan bencana yang kukuh untuk melindungi data organisasi dalam kejadian insiden yang merugikan. g) Menilai semula keselamatan maklumat secara berkala dan memastikan ia selaras dengan keperluan keselamatan dan piawaian. h) Memastikan bahawa organisasi mematuhi peraturan dan perundangan yang berkaitan dengan penggunaan perkhidmatan awan, terutamanya dalam hal privasi data dan perlindungan data peribadi; i) Mewujudkan prosedur Pengurusan Pengkomputeran Awan.	

5.24	**Perancangan, Penyediaan Dan Pengurusan Insiden Keselamatan Maklumat (*Information Security Incident Management Planning And Preparation*)**
Objektif: Memastikan insiden keselamatan ICT dan kelemahan dilapor dan di salur dengan cepat dan berkesan bagi meminimumkan proses pembaikan dan mengurangkan kesan insiden keselamatan ICT.	
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan,	**Pengarah DTM, ICTSO**

kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada MBSA. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Tindakan menangani insiden keselamatan ICT perlu dilakukan dengan cepat, teratur dan berkesan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:- a. Mengenal pasti jenis insiden keselamatan ICT; b. Menyimpan jejak audit, sandaran (backup) secara berkala dan melindungi integriti semua bahan bukti; c. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; d. Menyediakan, melaksanakan dan menyelenggara pelan Kesinambungan Perkhidmatan dan mengaktifkan pelan tersebut; e. Menyediakan tindakan pemulihan segera; f. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu; g. Memberikan kesedaran berkaitan Prosedur Pengurusan Insiden Keselamatan ICT dan hebahan kepada warga MBSA sekiranya terdapat pindaan; dan h. Memastikan pegawai bertanggungjawab menguruskan insiden mempunyai tahap kompetensi yang diperlukan.	

5.25	**Penilaian Dan Keputusan Peristiwa Keselamatan Maklumat (*Assessment And Decision On Information Security Events*)**

Objektif:

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

Insiden keselamatan maklumat hendaklah dinilai dan ditentukan	**ICTSO**

jika ia perlu dikelaskan sebagai insiden keselamatan maklumat. Penilaian ini bertujuan untuk memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT Majlis Bandaraya Shah Alam (MBSA). Antara jenis situasi insiden yang terlibat adalah: a. Maklumat didapati hilang 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; 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.	

5.26	**Maklum balas Insiden Keselamatan Maklumat (*Respon To Information Security Incident*)**
Objektif: Memastikan tindakan terhadap insiden keselamatan ICT dapat dilaksanakan dengan berkesan.	
Insiden keselamatan maklumat hendaklah ditangani berdasarkan Prosedur Pengurusan Insiden Keselamatan ICT yang didokumenkan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut: 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	**ICTSO**

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. Memaklumkan atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	

5.27	**Pembelajaran Daripada Insiden Keselamatan Maklumat (*Learning From Information Security Incidents*)**
Pengetahuan yang diperolehi daripada analisa 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. Antara kawalan yang boleh diambil seperti a. Mewujudkan prosedur untuk mengukur dan memantau jenis, saiz dan kos kejadian; b. Menyediakan pelan kontigensi bagi mengawal kejadian insiden keselamatan berulang; c. Mengadakan latihan dan taklimat berkenaan dengan PKS MBSA.	**ICTSO**

5.28	**Pengumpulan Bukti (*Collection Of Evidence*)**
Objektif: Memastikan bukti insiden keselamatan ICT dapat direkod dan dianalisa bagi tujuan kegunaan pengesahan tindakan disiplin dan undang-undang.	
MBSA hendaklah menentukan prosedur untuk mengenai pasti koleksi, perolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan	**ICTSO**

semasa yang berkaitan. Memastikan pengurusan bukti yang konsisten dan berkesan berkaitan insiden IS untuk tujuan tindakan tatatertib dan undang-undang. Membangunkan prosedur dalaman dan menyediakan arahan untuk pengenalan, pengumpulan, perolehan dan pemeliharaan bukti. Bukti sepatutnya boleh ditunjukkan bahawa; a. rekod adalah lengkap dan tidak diusik dengan apa cara sekalipun; b. salinan bukti elektronik mungkin sama dengan yang asal; dan c. mana-mana sistem maklumat yang mana bukti telah dikumpulkan telah beroperasi dengan betul pada masa bukti direkodkan.	

5.29	**Keselamatan Maklumat Semasa Gangguan (*Information Security During Disruption*)**
Objektif: Memastikan maklumat dan aset berkaitan dalam keadaan selamat.	
5.29.1	**Pelan Kesinambungan Perkhidmatan**
Pelan Kesinambungan Perkhidmatan (*Business Continuity Plan - BCP*) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh pihak pengurusan MBSA. Perkara-perkara berikut perlu diberi perhatian: a. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan	**Pengarah DTM, Pemilik Sistem ICT**

kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT;

c. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;
d. Mendokumentasikan proses dan prosedur yang telah dipersetujui;
e. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;
f. Membuat *backup*; dan
g. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.

BCP mempunyai empat komponen utama iaitu:-

a. Pelan Pemulihan Bencana;
b. Pelan Tindak balas Kecemasan;
c. Pelan Tindak balas Insiden; dan
d. Pelan Komunikasi.

dan hendaklah mengandungi perkara-perkara berikut:

a. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
b. Senarai personel MBSA dan vendor berserta nombor yang boleh dihubungi (faks, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden;
c. Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;
d. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan
e. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh.

Salinan BCP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. BCP hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian BCP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. MBSA hendaklah memastikan salinan BCP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

5.29.2	***Backup* dan *Restore***

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, backup hendaklah dilakukan setiap kali konfigurasi berubah mengikut prosedur yang telah ditetapkan.

Perkara-perkara yang perlu dicontohi adalah seperti berikut :

a. Membuat backup keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;
b. Membuat backup ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan backup bergantung pada tahap kritikal maklumat;
c. Menguji sistem backup dan restore sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan sekurang-kurangnya 2 kali setahun;
d. Menyimpan sekurang-kurangnya tiga (3) generasi (backup); dan
e. Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat.

5.30	**Ketersediaan ICT Untuk Kesinambungan Perkhidmatan (*ICT Readiness For Business Continuity*)**

Objektif:
Memastikan maklumat dan aset berkaitan dalam keadaan selamat.

Teknologi Maklumat dan Komunikasi (ICT) adalah aspek penting dalam memastikan kesinambungan operasi organisasi. Ini	**Pengarah DTM,** **ICTSO,**

melibatkan penyediaan infrastruktur, sistem, dan perkhidmatan ICT yang boleh diakses dan berfungsi dengan baik dalam semua keadaan, termasuk semasa krisis atau gangguan. Faktor-faktor yang perlu dipertimbangkan untuk mencapai ketersediaan ICT bagi kesinambungan 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; 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 mengenalpasti masalah sebelum ia berlaku dan mengelakkan gangguan; f. Pengurusan inventori peralatan, pelan pembaikan, dan pemantauan prestasi berterusan. Sediakan pelan pemulihan bencana ICT yang komprehensif. Ini termasuk cadangan data, pengekalkan cadangan pelayan, dan satu prosedur pemulihan semula aktiviti perniagaan. a. Ujian dan latihan berkala pelan pemulihan bencana; b. Pastikan akses kepada sistem dan data dikawal dengan ketat dan disemak secara berkala. Ini termasuk pengurusan identiti, pengesahan dua faktor, dan peraturan akses yang ketat; c. Sediakan perkhidmatan pengurusan keselamatan seperti antivirus, firewall, dan pelindung kegagalan untuk	**Pentadbir Sistem ICT**

menghalang ancaman keselamatan ICT; d. Amalkan pemantauan keselamatan untuk mengenalpasti dan tindak balas kepada ancaman dan insiden keselamatan; e. Pastikan kakitangan tahu apa yang perlu dilakukan dalam kes insiden keselamatan; f. Melaksanakan penyelenggaraan dan pembaikan peralatan dan sistem secara berkala untuk mengelakkan kegagalan yang tidak dijangka; g. Tetapkan jadual pembaikan berkala dan pemulihan data; h. Pantau penggunaan sumber daya ICT seperti *bandwidth* dan kapasiti penyimpanan untuk mengelakkan penggunaan berlebihan yang boleh menyebabkan gangguan. Pastikan penyedia perkhidmatan awan atau penyedia perkhidmatan lain mempunyai pelan kesinambungan perniagaan yang mencukupi yang dapat menyokong operasi jika berlaku gangguan.	

5.31	**Pematuhan Terhadap Keperluan Perundangan, pekeliling, Peraturan dan Perjanjian Kontrak *(Legal, Statutory, Regulatory And Contractual Requirements)***
Objektif: Meningkat dan memantapkan tahap keselamatan siber bagi mengelak daripada pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.	

Faktor perundangan hendaklah dikenalpasti dan semua kakitangan terlibat wajib mematuhinya, pihak syarikat pembekal, pakar-pakar runding dan mana-mana pihak yang berurusan dengan pihak Majlis juga perlu mematuhi undang-undang dan peraturan yang diterima pakai. Senarai perundangan dan peraturan yang perlu dipatuhi adalah seperti di Lampiran 1. Semua keperluan undang-undang, peraturan dan kontrak yang berkaitan dengan MBSA perlu ditakrifkan, didokumenkan, dan disimpan sehingga tarikh yang sesuai bagi setiap maklumat. Semua keperluan perundangan, pekeliling dan peraturan adalah seperti di Lampiran 1. Perkara berkaitan perundangan yang perlu diberi perhatian adalah seperti berikut: a. Setiap pengguna hendaklah membaca, memahami dan mematuhi PKS MBSA dan undang-undang atau peraturan-peraturan lain berkaitan yang berkuatkuasa; b. Semua perjanjian dan pekeliling berkaitan ICT termasuk maklumat yang disimpan di dalamnya adalah hakmilik MBSA dan Ketua Jabatan berhak memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan; c. Sebarang penggunaan aset MBSA selain daripada maksud dan tujuan yang telah ditetapkan adalah merupakan satu penyalahgunaan sumber MBSA.	**Kakitangan Majlis dan syarikat-syarikat yang berurusan secara rasmi dengan pihak Majlis**

5.32	**Hak Harta Intelek** ***(Intellectual Property Rights)***
Hak Harta Intelek Majlis perlu dilindungi melalui penguatkuasaan perundangan dan peraturan yang telah ditetapkan. Data-data dan dokumen yang digunapakai perlu dipastikan asli dan tidak diambil daripada harta intelek pihak lain. Semua aplikasi yang digunakan hendaklah yang asli (*genuine*).	**Kakitangan Majlis dan pihak syarikat yang berurusan secara rasmi dengan Majlis**

5.33	**Perlindungan Rekod (*Protection of Records)***

Objektif:

Memastikan pematuhan kepada keperluan undang-undang, berkanun, peraturan dan kontrak, serta jangkaan komuniti atau masyarakat yang berkaitan dengan perlindungan dan ketersediaan rekod.

Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak seperti Akta Arkib Negara, Arahan Keselamatan dan Garis Panduan Keselamatan Maklumat Terbitan 2023.	**Semua**

5.34	**Privasi dan Perlindungan Maklumat Pengenalan Peribadi (*Privacy and Protection of Personal Identifiable Information* (PII))**

Objektif:

Memberikan jaminan dalam melindungi maklumat peribadi pengguna.

Maklumat peribadi pengguna hendaklah dilindungi sebaiknya oleh pihak Majlis. Kawalan yang ketat perlu dilaksanakan agar maklumat tidak mudah diberikan kepada pihak lain mengikut perundangan dan peraturan yang ditetapkan seperti yang dinyatakan di dalam Panduan Data Peribadi Sektor Awam yang terkini.	**Kakitangan Majlis dan pihak syarikat yang berurusan secara rasmi dengan Majlis**

5.35	**Semakan Semula Keselamatan Maklumat (*Independent Review Of Information Security*)**

Objektif:

Mengkaji kesesuaian, kecukupan dan keberkesanan pengurusan keselamatan maklumat organisasi.

Penilaian keselamatan maklumat oleh organisasi hendaklah dilaksanakan secara berkala seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur melalui audit dalaman dan luaran.	**Pengarah DTM, ICTSO**

5.36	**Pematuhan Polisi, Peraturan dan Piawaian Keselamatan Maklumat (*Compliance With Policies, Rules, and Standards for Information Security*)**

Objektif:

Memastikan pengurusan keselamatan maklumat organisasi adalah beroperasi berdasarkan kepada polisi, peraturan dan standard yang ditetapkan.

Memastikan semua warga MBSA dan pihak ketiga yang berkaitan mematuhi semua polisi, peraturan dan piawaian keselamatan maklumat yang ditetapkan. Sebarang ketidakpatuhan polisi, peraturan dan piawaian keselamatan maklumat tindakan tatatertib boleh diambil mengikut kesalahan.	**Warga MBSA, Pihak Ketiga**

5.37	**Prosedur Operasi Yang Didokumenkan (*Documented Operating Procedure*)**

Objektif:

Memastikan prosedur operasi diwujudkan dan di dokumentasikan.

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, Pentadbir Sistem ICT**

PERKARA	PERANAN
ANNEX 6 – KAWALAN MANUSIA (*PEOPLE CONTROLS*)	
Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan MBSA, pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga MBSA hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.	

6.1	Saringan (*Screening*)	
	Tapisan keselamatan hendaklah dijalankan terhadap calon pekerja Majlis terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan MBSA serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b) Menjalankan tapisan keselamatan, semakan latar belakang, pendidikan untuk calon pekerja serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; d) penentuan calon temuduga - sesi tapisan bersama Bahagian Integriti, Perundangan dan Jabatan berkaitan; e) Semakan nama yang layak di temuduga di hantar ke SPRM, PDRM dan AADK untuk semakan sekiranya ada kes. c) Menjalankan Ujian Fizikal bagi jawatan-jawatan tertentu seperti Pembantu Penguatkuasa, Pengawal Keselamatan dan Pengawal;	**Jabatan Khidmat Pengurusan dan Semua**

d) Menjalankan "Urine Test" kepada calon yang layak di temuduga (sekiranya perlu); e) Menjalankan ujian kompetensi bagi jawatan pemandu kenderaan; f) Menjalankan pemeriksaan kesihatan menyeluruh bagi kakitangan berumur 35 hingga 60 tahun; g) Memenuhi syarat dan kriteria pengambilan dengan merujuk terma dan syarat setiap jawatan yang diiklankan; h) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan. Rujuk kepada Prosedur Pengambilan dan Pengisian Kakitangan.	

6.2	**Terma Dan Syarat Pekerjaan (*Terms And Condition Employment*)**	
Memastikan semua pihak memahami tanggungjawab ke atas keselamatan maklumat berdasarkan peranan mereka di organisasi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut:- a) Memastikan pegawai dan kakitangan MBSA serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh MBSA; b) Kakitangan yang dilantik diberi surat tawaran dan perjanjian (Kakitangan Kontrak) yang menerangkan peraturan-peraturan dan syarat-syarat Majlis dan Kerajaan dari semasa ke semasa; c) Kakitangan yang baru dilantik perlu menandatangani : i) Borang Penerimaan Jawatan ii) Borang Aku Janji iii) Borang Akta Rahsia Rasmi iv) Borang Aku Janji DKICT/PKS		**Jabatan Khidmat Pengurusan dan Semua**

d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Seksyen Latihan & Strategik, Jabatan Khidmat Pengurusan MBSA.	

6.3	**Kesedaran Keselamatan Maklumat, Pendidikan Dan Latihan (*Information Security Awareness Education and Training*)**
a) Setiap pengguna di MBSA perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden juga adalah penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT MBSA. b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MBSA secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari masa ke semasa; c) **Setiap lantikan kakitangan baru akan diberi taklimat berkaitan polisi keselamatan siber. Manakala bagi kakitangan MBSA sedia ada , Seksyen Latihan & Strategik akan merancang untuk membuat Taklimat bersiri.** Rujukan bagi pelaksanaan **KESEDARAN KESELAMATAN MAKLUMAT, PENDIDIKAN DAN LATIHAN (INFORMATION SECURITY AWARENESS AND TRAINING) adalah dengan menggunakan Pelan Operasi dan TNA.**	**Jabatan Khidmat Pengurusan, JDTM**

6.4	Proses Tindakan Tatatertib (*Disciplinary Process*)	
	Proses tindakan disiplin dan / atau undang-undang ke atas pegawai dan kakitangan MBSA serta pihak ketiga yang berkepentingan perlu diambil sekiranya berlaku pelanggaran dengan perundangan dan peraturan yang ditetapkan oleh MBSA. Prosedur proses tindakan tatatertib telah diwujudkan yang melibatkan beberapa langkah utama yang mana boleh dirujuk adalah seperti yang berikut: **a) Pembangunan Dasar:** Bahagian Integriti perlu menentukan peraturan, dasar dan jangkaan yang jelas untuk tingkah laku di tempat kerja atau organisasi. Ianya harus dimaklumkan dengan menyampaikan secara berkesan kepada semua kakitangan MBSA. **b) Dokumentasi:** Terdapat proses yang jelas untuk mendokumentasikan insiden salah laku atau pelanggaran dasar yang berlaku di Majlis. Bahagian Integriti akan menggunakan **Akta Kerajaan Tempatan 1976 Kaedah - Kaedah Pegawai Majlis Bandaraya Shah Alam (Kelakuan dan Tatatertib) 2023** sebagai rujukan bagi proses tindakan tatatertib yang berlaku di Majlis. **c) Penyiasatan:** Prosedur untuk menyiasat insiden yang dilaporkan adalah dengan mengadakan temu bual saksi, mengumpul bukti, dan mendokumentasikan penemuan secara berekod. d) **Keadilan:** Bahagian Integriti perlu menekankan keadilan dan konsistensi sepanjang proses. Layanan kepada semua pekerja sama rata dan pastikan tindakan tatatertib yang diambil adalah berdasarkan bukti dan dasar yang terpakai. **e) Komunikasi:** Menyampaikan dengan jelas proses tindakan tatatertib yang akan diambil kepada kakitangan, termasuk surat dan memo	**Bahagian Integriti** **Seksyen Sumber Manusia,** **Jabatan Khidmat Pengurusan**

panggilan kepada kakitangan serta pelaksanaan siasatan dalaman bagi insiden yang berlaku. **f) Disiplin Progresif:** Bahagian Integriti akan melaksanakan pendekatan disiplin secara progresif, dimana akibatnya akan meningkat bagi setiap pelanggaran yang berulang. Tindakan ini akan diambil secara berperingkat dengan mengeluarkan amaran lisan, surat tunjuk sebab, penggantungan, penahanan dan penamatan.	

6.5	**Tanggungjawab Selepas Penamatan Atau Perubahan Pekerjaan (*Responsibilities After Termination or Change of Employment*)**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut:- a) Memastikan semua aset ICT dikembalikan kepada MBSA mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; b) Penamatan Perkhidmatan/ Peletakan Jawatan i. Borang Akuan Pemulangan perlu dipulangkan dan disertakan bersekali dengan Pas Pekerja, Kad Akses Masuk/Keluar Wisma dan Kad Kuasa (Jika ada); ii. Borang Perakuan apabila meninggalkan perkhidmatan Awam (perlu diisi sekiranya mendapatkan tawaran selain agensi Kerajaan) Lampiran E; iii. Borang Pendaftaran dan Penamatan Akaun Pengguna (MBSA-ISMS-ICT-PO-02-01). Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh MBSA dan / atau terma perkhidmatan; iv. Bertanggungjawab menguruskan segala tanggungan hutang dengan MBSA dan Kerajaan. c) Persaraan Wajib/ Paksa i. Mengembalikan Pas Pekerja, Kad Akses Masuk/Keluar	**Semua,** **Jabatan Khidmat Pengurusan,** **JDTM**

Wisma dan Kad Kuasa (Jika ada); ii. Borang Pendaftaran dan Penamatan Akaun Pengguna (MBSA-ISMS-ICT-PO-02-01). Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh MBSA dan / atau terma perkhidmatan; iii. Menandatangani Borang Perakuan untuk ditandatangani apabila meninggalkan perkhidmatan Kerajaan (Lampiran E); iv. Bertanggungjawab menguruskan segala tanggungan hutang dengan MBSA dan Kerajaan.	

6.6	**Kerahsiaan Atau Perjanjian Bukan Pendedahan (*Confidentiality Or Non-Disclosure Agreements*)**
Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan di dokumentasikan. Kakitangan MBSA yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972. Setiap pegawai dan kakitangan MBSA perlu mengisi Perakuan berkenaan Akta Rahsia Rasmi 1972 setiap tahun.	**Jabatan Khidmat Pengurusan dan Semua**

6.7	**Bekerja Luar Pejabat (*Remote Working*)**
Memastikan keselamatan maklumat terjamin apabila terdapat kakitangan bekerja dari luar pejabat yang memerlukan capaian jarak jauh. Perkara-perkara yang perlu dipatuhi termasuk yang berikut:- **i. Dasar dan Garis Panduan:** MBSA telah menggunapakai Pekeliling Perkhidmatan Bilangan 5 Tahun 2020 – Dasar Bekerja Dari Rumah.	**Semua**

ai. Teknologi dan Infrastruktur: Memastikan pekerja mempunyai akses yang mencukupi dan selamat kepada teknologi yang diperlukan, seperti komputer, perisian, capaian internet pantas dan peranti keselamatan seperti VPN (Virtual Private Network) jika perlu. **bi. Komunikasi Berkesan:** Wujudkan alat komunikasi yang berkesan untuk memudahkan kerjasama antara pasukan yang bekerja dari jauh, seperti e-mel, 'Whatsapp', 'Telegram', persidangan video dan alatan kerjasama dalam talian seperti Google Meet. **iv. Pengurusan Keselamatan Maklumat:** Pastikan sistem dan data Majlis kekal selamat apabila pekerja bekerja dari jauh. Laksanakan langkah keselamatan maklumat, seperti akses terhad.\ **v. Fleksibiliti** MBSA melaksanakan Waktu Bekerja Fleksi dengan waktu bekerja dari jam 7.30 pagi hingga 6.00 petang. Kakitangan yang diluluskan Bekerja Dari Rumah perlu merakam kehadiran dengan menggunakan Sistem Online yang digunapakai.	

6.8	**Pelaporan Keselamatan Maklumat (*Information Security Event Reporting*)**
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada	**ICTSO**

MBSA.

Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Tindakan menangani insiden keselamatan ICT perlu dilakukan dengan cepat, teratur dan berkesan.

Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:-

a) Mengenal pasti jenis insiden keselamatan ICT;
b) Menyimpan jejak audit, sandaran (*backup*) secara berkala dan melindungi integriti semua bahan bukti;
c) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;
d) Menyediakan, melaksanakan dan menyelenggara pelan Kesinambungan Perkhidmatan dan mengaktifkan pelan tersebut;
e) Menyediakan tindakan pemulihan segera; dan
f) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.

Prosedur pelaporan insiden keselamatan ICT berdasarkan:-

- *Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi;* dan
- *Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam*

PERKARA		PERANAN
ANNEX 7 – KAWALAN FIZIKAL (*PHYSICAL* CONTROLS)		
7.1	**Perimeter Keselamatan Fizikal (*Physical Security Perimeters*)**	
Objektif: Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman dan kerosakan.		
Kawalan fizikal kawasan adalah bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi dengan mengesan dan mencegah cubaan menceroboh. Antara langkah-langkah keselamatan fizikal adalah:- a. Lokasi hendaklah dikenal pasti dengan jelas; b. Lokasi hendaklah diperkukuhkan seperti dinding, siling, tingkap dan pintu serta dikunci untuk mengawal kemasukan; c. Memasang alat penggera atau kamera tertutup; d. Menghadkan jalan keluar masuk; e. Mengadakan kaunter kawalan; f. Menyediakan tempat atau bilik khas 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. Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan tempat-tempat yang memerlukan kawalan; j. Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; k. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan		**Datuk Bandar, CIO, Penguatkuasa / JKP / Korporat / JDTM**

l. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	

7.2	**Kemasukan Fizikal (*Physical Entry*)**	
Objektif: Melindungi premis dan aset ICT daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.		
7.2.1	**Kawalan Masuk Fizikal**	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut:- a. Setiap warga kerja MBSA hendaklah memakai atau mengenakan pas pekerja sepanjang waktu bertugas; a. Setiap pelawat hendaklah mendaftar dan mendapatkan pas pelawat di lobi dan pas dikembalikan semula selepas selesai urusan; b. Semua pas pekerja hendaklah diserahkan balik kepada Bahagian Sumber Manusia, Jabatan Khidmat Pengurusan apabila kakitangan berhenti atau bersara; dan c. Kehilangan pas mestilah dilaporkan dengan segera d. Semua kawasan larangan dipasang terminal akses kad		**Semua**
7.2.2	**Keselamatan Persekitaran**	
Melindungi aset MBSA dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.		**Semua**
7.2.3	**Kawalan Kawasan Penghantaran Barangan dan *Loading Area***	
Kawasan penghantaran barangan dan *loading* area hendaklah dikawal dan perlu dipisahkan dari akses terus ke kawasan larangan.		**JKP / Penguatkuasa**

7.3	**Keselamatan Pejabat, Bilik, Dan Kemudahan (*Securing Offices, Rooms And Facilities*)**	
Objektif: Melindungi premis dan aset MBSA daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.		
Kawasan larangan ditakrifkan sebagai kawasan yang aksesnya dihadkan kepada pegawai-pegawai yang diberi kuasa sahaja. Ini dilaksanakan untuk melindungi aset MBSA yang terdapat di dalam kawasan tersebut. Kawasan larangan di MBSA adalah bilik Datuk Bandar, Bilik Timbalan Datuk Bandar, bilik-bilik Pengarah dan Pegawai, Bilik Fail, Pusat Data Bilik Server, *Disaster Recovery Centre* (DRC) dan Pusat Kawalan CCTV (IRIS) serta mana-mana kawasan yang telah / akan diisytiharkan sebagai kawasan larangan. Akses kepada bilik-bilik tersebut adalah terhad kepada pegawai-pegawai yang diberi kuasa sahaja.	**Semua**	

7.4	**Pemantauan Keselamatan Fizikal *(Physical Security Monitoring)***	
Objektif: Melindungi premis dan aset MBSA daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan		
Akses tanpa kebenaran ke kawasan fizikal terhad seperti bilik pelayan (server) dan bilik peralatan IT boleh mengakibatkan kehilangan kerahsiaan, ketersediaan, integriti dan keselamatan aset maklumat. Berikut adalah kawalan yang boleh dilaksanakan: a. Pemasangan Kamera CCTV di ruang dan perkarangan pejabat; b. Mengadakan Pengawal keselamatan di pos masuk utama; c. Menghadkan kawalan masuk di Pusat Data, Pusat Pemulihan Data dan Bilik Server dan terhad kepada pegawai yang diberi kebenaran. Bagi kemasukan servis provider ke kawasan tersebut perlu direkodkan di dalam buku rekod keluar/masuk pusat data dan diiringi oleh pegawai ICT yang berkenaan; d. Pemantauan kad akses melalui sistem yang disediakan; e. Pendaftaran pelawat di pintu masuk utama.	**Semua**	

7.5	**Perlindungan Fizikal Dan Ancaman Persekitaran** ***(Protection Against Physical And Environmental Threats)***

Objektif:

Melindungi aset MBSA dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset MBSA, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada CIO. Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi:- a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan keselamatan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset MBSA; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset MBSA; f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; g. Semua peralatan perlindungan hendaklah disemak dan diuji secara berkala. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan h. Akses kepada saluran *riser* hendaklah sentiasa berkunci. i. Kawalan serangga perosak dijalankan secara berkala	**Semua**

7.6	**Bekerja Di Kawasan Yang Selamat** ***(Working In Secure Area)***

Objektif:

Melindungi premis dan aset MBSA daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan

7.6.1	**Kawasan Larangan**	
Sumber data atau pelayan (*server*), peralatan komunikasi dan storan perlu ditempatkan di Pusat Data, Disaster Recovery Centre (DRC), bilik pelayan (*server*) atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegah kebakaran; a. Pemantauan dibuat menggunakan kamera *CCTV* atau lain-lain peralatan yang sesuai; b. Peralatan keselamatan (*CCTV*, log akses) perlu diperiksa secara berjadual; c. Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; d. Pelawat yang dibawa masuk mesti diiringi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; e. Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan dan laluan awam; f. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; g. Memperkukuhkan dinding dan siling; h. Menghadkan jalan keluar masuk; i. Menyediakan tempat atau bilik khas untuk pelawat; j. Peralatan ICT di dalam kawasan larangan hendaklah dijaga dan dikawal supaya sentiasa dalam keadaan selamat, baik dan boleh digunakan. k. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan, kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan l. Semua penggunaan peralatan yang melibatkan	**Semua**

penghantaran, pengemaskinian dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Pengarah Jabatan / Ketua Bahagian / Pengurus Pejabat Cawangan.	

7.7	**Dasar Meja Kosong Dan Skrin Kosong** ***(Clear Desk And Clear Screen)***

Objektif:

Mengurangkan risiko capaian yang tidak dibenarkan ke atas maklumat semasa dan di luar waktu kerja biasa.

Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja atau di paparan skrin apabila kakitangan tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a. Menggunakan kemudahan password screen saver atau logout apabila meninggalkan komputer; b. Pengguna perlu *lock screen* apabila meninggalkan komputer pada bila-bila masa~~,~~ jika tidak screen akan dilock selepas lima belas (15) minit *idle*;~~–~~ c. Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci apabila meninggalkan meja kerja; dan d. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	**Semua**

7.8	**Lokasi Dan Perlindungan Peralatan** ***(Equipment Siting And Protection)***

Objektif:

Melindungi peralatan ICT MBSA dari kehilangan dan perkara-perkara yang boleh membahayakan.

Dalam memastikan peralatan ICT dikawal dan dijaga dengan baik, perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a) Pengguna hendaklah bertanggungjawab menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; b) Pengguna hendaklah memastikan semua perkakasan disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; c) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran dan tidak digunakan untuk tujuan peribadi; d) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan serta membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem Aplikasi; e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f) Pengguna mesti memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; h) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem Aplikasi atau Juruteknik untuk di baik pulih; i) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable*	**Semua**

Power Supply (*UPS*); j) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; l) Peralatan ICT yang hendak dibawa keluar dari premis MBSA, perlulah mendapat kelulusan Pentadbir Sistem Aplikasi dan direkodkan bagi tujuan pemantauan; m) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera; n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset ICT; p) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; q) Konfigurasi alamat *IP* tidak dibenarkan diubah daripada alamat *IP* yang asal; r) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Sistem Aplikasi / Juruteknik. Kata laluan bagi pentadbir (*administrator password*) adalah terhad untuk pengetahuan pentadbir sistem sahaja. Selain itu, kata laluan ini juga perlu dicipta berdasarkan saranan polisi umum bagi kata laluan agar ianya kukuh dan tidak mudah diketahui oleh pihak lain. Kata laluan ini juga hendaklah diubah secara berkala bagi mengelakkan kebocoran yang tidak diingini; s) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; t) Pengguna hendaklah memastikan semua perkakasan komputer,	

pencetak dan pengimbas dimatikan apabila meninggalkan pejabat; u) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; v) Memastikan soket dimatikan daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya; dan **w)** Memastikan setiap pemasangan aplikasi ataupun perisian hendaklah direkodkan, dan aplikasi ataupun perisian harus diuji dan dikemaskini sebelum dipasang dalam sistem *live* (*production*).	

7.9	**Keselamatan Aset Di Luar Premis** ***(Security Of Assets Off Premises)***
Objektif: Mengelakkan kehilangan, kerosakan, kecurian atau gangguan kepada operasi organisasi.	
Langkah-langkah yang perlu dipatuhi bagi perkakasan yang dibawa keluar dari permis MBSA adalah seperti di bawah:- a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan; b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan; c. Peralatan perlu dilindungi dan dikawal sepanjang masa; d. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian dan sebarang kehilangan peralatan adalah di bawah tanggungjawab individu yang membawa keluar peralatan tersebut; dan e. Kehilangan sebarang peralatan yang dibawa keluar hendaklah dimaklumkan segera kepada Pegawai Aset Majlis;	**Semua**

f. Permohonan akses VPN perlu direkodkan.	

7.10	Media Storan (*Storage Media*)

Objektif:

Memastikan agar pengubahsuaian, penyingkiran atau pemusnahan maklumat pada storan media dilaksanakan sewajarnya.

Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti cakera padat, *thumb drive,* pengkomputeran awan dan media storan lain. Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat:- a. Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja; c. Bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu; d. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu dan dihapuskan dengan teratur dan selamat; e. Pergerakan media storan hendaklah direkodkan; f. Pengguna bertanggungjawab terhadap keselamatan maklumat dalam storan mudah alih seperti *thumb drive* atau *external hard disk*; g. Perkakasan sandaran (*backup*) hendaklah diletakkan di tempat yang terkawal. Storan dan peralatan sandaran (*backup*) hendaklah disimpan di lokasi yang berasingan dan tidak terbuka kepada umum atau mengikut keperluan;	**Semua**

h. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; i. Mengadakan salinan atau sandaran (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; j. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur k. dan selamat.	

7.11	UTILITI SOKONGAN (*SUPPORTING UTILITIES*)
Objektif: Memastikan agar peralatan dan perkakasan yang memproses maklumat dapat dilindungi dari terputusnya bekalan kuasa.	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. 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 bilik pelayan (*server*) supaya mendapat bekalan kuasa berterusan; dan c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	**Kejuruteraan, JDTM**

7.12	Keselamatan Kabel *(Cabling Security)*
Objektif: Memastikan segala jenis kabel yang digunakan dalam operasi harian keselamatan maklumat telah dilindungi dari ancaman.	

Kabel komputer hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah:- 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 terutamanya daripada kerosakan dan pintasan maklumat. e. Akses kepada saluran *riser* hendaklah sentiasa berkunci.	**Kejuruteraan, JDTM**

7.13	**Penyelenggaraan Perkakasan (*Equipment Maintenance*)**
Objektif: Perkakasan ICT hendaklah diselenggara mengikut jadual bagi memastikan ianya *Confidentiality*, *Integrity* dan *Accessebility* (CIA) dan di dalam keadaan selamat.	
Perkakasan hendaklah diselenggara agar tidak bermasalah bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan; b. Perkakasan hanya boleh diselenggara 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. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; e. Peralatan pengukuran mestilah ditentukur dalam jangka masa yang telah ditetapkan;	**JDTM / Penguatkuasa / Kejuruteraan**

f. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan g. Semua penyelenggaraan mestilah mendapat kebenaran daripada pegawai.	

7.14	**Pelupusan Selamat Atau Penggunaan Semula Peralatan (*Secure Disposal Or Re-Use Of Equipment*)**
Objektif: Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MBSA dan ditempatkan di MBSA.	
Peralatan ICT yang hendak dilupuskan atau diguna semula terutama yang mengandungi maklumat terperingkat atau perisian yang dilesenkan, perlu diuruskan dengan teratur dan selamat melalui prosedur pelupusan semasa atau guna semula peralatan yang telah ditetapkan. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MBSA. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh diguna semula atau dilupuskan; b. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum diguna semula atau pelupusan dilakukan; c. Peralatan ICT yang akan dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; e. Peralatan ICT hendaklah di *format* atau diubah kepada keadaan asal *(set to factory setting)* sebelum diguna semula atau dilupuskan. f. Peralatan yang hendak dilupus hendaklah disimpan di	**Semua**

tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;

g. Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan; dan
h. Pelupusan oleh pihak ketiga hendaklah dilakukan mengikut tatacara pelupusan dan menyediakan bukti penyaksian pelupusan;

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

a. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk menjadi milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman *CPU* seperti *RAM, hard disk, motherboard, modem* dan sebagainya;
b. Menyimpan dan memindahkan perkakasan luaran komputer seperti *AVR, speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di MBSA;
c. Memindah keluar dari MBSA mana-mana peralatan ICT yang hendak dilupuskan;
d. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab MBSA;
e. Semua kakitangan bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan; dan
f. Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana *Arahan Keselamatan* dan *Tatacara Jabatan Arkib Negara*.

PERKARA	PERANAN
ANNEX 8 – KAWALAN TEKNOLOGI (*TECHNOLOGICAL CONTROLS*)	

8.1	**Peranti Akhir Pengguna** ***(User End Point Devices)***
Objektif: Melindungi maklumat yang disimpan, diproses dan dicapai daripada sebarang bentuk pencerobohan, ancaman dan kerosakan melalui peranti akhir pengguna.	
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. Peralatan mudah alih yang dikhaskan untuk pegawai yang berkelayakan dibenarkan dibawa keluar bagi melaksanakan tugas-tugas rasmi; b. Peralatan mudah alih gunasama perlu direkod dan mendapat kelulusan pegawai yang bertanggungjawab apabila hendak dibawa keluar dari pejabat; c. Semua peralatan mudah alih hendaklah dilindungi dan dikawal dengan selamat; d. Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan. *e. Peralatan BYOD perlu mengikut mengikut Garis panduan BYOD MBSA;* f. Tamatkan sesi aktif apabila selesai tugas; dan g. *Log-off* komputer meja dan komputer riba apabila sesi bertugas selesai;	**Semua**

8.2	**Hak Capaian Istimewa** ***(Privileged Access Rights)***
Objektif: Memastikan hanya pengguna yang dibenarkan, komponen perisian dan perkhidmatan disediakan diberi hak capaian istimewa.	
Hak capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada.	Semua

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: c) Kawalan capaian ke atas Aset ICT mengikut keperluan keselamatan dan peranan pengguna; d) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; e) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan f) Kawalan ke atas kemudahan pemprosesan maklumat.	
8.2.1	**Akaun Pengguna**
Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, Pentadbir Sistem perlu mengambil langkah-langkah berikut:- a) Akaun yang diperuntukkan oleh MBSA sahaja boleh digunakan; b) Akaun pengguna (*user id*) hendaklah unik; c) Pemilik akaun pengguna bukanlah hak mutlak pengguna dan ia tertakluk kepada peraturan MBSA. Akaun boleh ditarik balik jika pengguna melanggar peraturan; d) Tidak semua pengguna boleh mencapai semua peringkat maklumat. Terdapat peringkat dalam capaian maklumat dengan dikawal menggunakan akaun. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f) Akaun pengguna boleh dibekukan dan ditamatkan atas sebab-sebab berikut:- a. Bertukar bidang tugas kerja; b. Bertukar ke agensi lain; c. Bersara; d. Digantung perkhidmatan ; atau e. Ditamatkan perkhidmatan	**Semua**
8.2.2	**Hak Capaian**
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	**Pentadbir Sistem Aplikasi**
8.2.3	**Pengurusan Kata Laluan**
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh	**Pentadbir Sistem Aplikasi Dan**

MBSA seperti berikut:- i. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; ii. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau di kompromi; iii. Panjang kata laluan disyorkan sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus; iv. Kata laluan hendaklah diingati dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; v. Kata laluan *windows* dan *screen saver* disyorkan diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; vi. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; vii. Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas kata laluan di set semula; viii. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; ix. Disyorkan had masa pengesahan selama dua (2) minit / mengikut kesesuaian sistem dan selepas had itu, sesi ditamatkan; x. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan xi. Mengelakkan penggunaan semula kata laluan yang baru digunakan. xii. Kata laluan asal (*default password*) mesti ditukarkan selepas pemasangan perisian atau perkakasan baru.	**Semua**
8.2.4	***Clear Desk dan Clear Screen***
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja atau di paparan skrin apabila kakitangan tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Gunakan kemudahan *password*; b) Log keluar apabila meninggalkan komputer; c) Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci; dan d) Memastikan semua dokumen diambil segera dari pencetak,	**Semua**

pengimbas, mesin faksimile dan mesin fotostat.		
8.2.5	**Capaian Rangkaian**	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:- i. Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MBSA, rangkaian agensi lain dan rangkaian awam; ii. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan iii. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.		**ICTSO Dan Pentadbir Sistem Aplikasi**
8.2.6	**Capaian Internet**	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- i. Penggunaan Internet di MBSA hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, *virus* dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MBSA; ii. Kaedah *Content Filtering* boleh digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; iii. Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; iv. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengarah DTM berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; v. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pengarah/ pegawai yang diberi kuasa; vi. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; vii. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah / Ketua Bahagian / Pengurus Pejabat Cawangan sebelum dimuat naik ke Internet; viii. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;		**Pengarah DTM Dan Ketua Seksyen Operasi & Teknikal**

ix. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MBSA; x. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; xi. Penggunaan *modem* atau '*broadband'* untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan xii. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:- a. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan b. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah. Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada *Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003* bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*".	
8.2.7	**Capaian Sistem Pengoperasian**
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi:- i. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; ii. Merekodkan capaian yang berjaya dan gagal; dan Kaedah-kaedah yang digunakan hendaklah menyokong perkara-perkara berikut:- i. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan; ii. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*; iii. Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem; dan iv. Menyediakan tempoh penggunaan mengikut kesesuaian.	**ICTSO Dan Pentadbir Sistem Aplikasi**

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- i. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; ii. Mewujudkan satu pengenalan diri (*ID*) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; iii. Menghadkan dan mengawal penggunaan program; dan iv. Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
8.2.8	**Kad Pintar**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- i. Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; ii. Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; iii. Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan disyorkan untuk disekat; dan iv. Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada DTM, MBSA.	**ICTSO Dan Pentadbir Sistem Aplikasi**
8.2.9	**Capaian Maklumat Dan Sistem Aplikasi**
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi:- i. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; ii. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); iii. Menghadkan capaian sistem dan aplikasi kepada minima tiga (3) kali percubaan adalah disyorkan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; iv. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan	**ICTSO Dan Pentadbir Sistem Aplikasi**

aktiviti atau capaian yang tidak sah; dan v. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah dibenarkan dengan kelulusan ICTSO. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	
8.2.10	**Peralatan Mudah Alih dan Kerja Jarak Jauh**
Peraturan-peraturan yang perlu dipatuhi bagi penggunaan mudah alih dan kerja jarak jauh adalah seperti berikut: i. Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan. ii. Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	**Semua**

8.3	**Sekatan Capaian Maklumat (*Information Access Restriction*)**
Objektif ; Memastikan hanya capaian yang dibenarkan dan menghalang capaian yang tidak dibenarkan ke atas maklumat dan lain-lain aset berkaitan (rangkaian atau sistem).	
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: i. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang diberikan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; ii. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); iii. Menghadkan capaian sistem dan aplikasi kepada minima tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; iv. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi	Semua

mengelakkan aktiviti atau capaian yang tidak sah; dan v. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah dibenarkan dengan kelulusan ICTSO. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja. vi. Semua sistem yang mendatangkan risiko yang tinggi kepada operasi MBSA perlu di asingkan daripada capaian terus melalui internet. vii. Pengasingan kepada sistem-sistem ini perlu dilaksana dengan menggunakan VLAN/VPN dan zon rangkaian (intranet, DMZ, internet)	

8.4	**CAPAIAN KEPADA KOD SUMBER (*ACCESS TO SOURCE CODE*)**

Objektif:

Untuk mengelakkan pengenalan fungsi yang tidak dibenarkan, elakkan perubahan yang tidak disengajakan atau berniat jahat dan untuk mengekalkan kerahsiaan harta intelek yang berharga.

Capaian kepada kod sumber hendaklah dihadkan Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- 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 agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan Sahaja bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; d) Capaian kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e) Menghalang sebarang peluang untuk membocorkan maklumat. f) Log audit perlu dikekalkan kepada semua akses kepada kod	**Pemilik Sistem dan** **Pentadbir Sistem Aplikasi**

	sumber	
8.4.1	**Pembangunan Perisian Secara *Outsource***	
Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik MBSA.		**JDTM dan** **Pentadbir Sistem Aplikasi**
8.4.2	**Kawalan Fail Sistem**	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem Aplikasi atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.		**Pemilik Sistem dan** **Pentadbir Sistem Aplikasi**

8.5	**Pengesahan Keselamatan (*Secure Authentication*)**
Objektif: Memastikan pengguna yang ditentusahkan sahaja yang dibenarkan mencapai aset ICT serta aplikasi sistem.	
Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, Pentadbir Sistem perlu mengambil langkah-langkah berikut:- a) Akaun yang diperuntukkan oleh MBSA sahaja boleh digunakan b) Mewujudkan teknik pengesahan samaada melalui 1 atau 2 faktor pengesahan mengikut kesesuaian sistem. c) Akaun pengguna (*user id*) hendaklah unik; d) Pemilik akaun pengguna bukanlah hak mutlak pengguna dan ia tertakluk kepada peraturan MBSA. Akaun boleh ditarik balik jika pengguna melanggar peraturan; e) Tidak semua pengguna boleh capai semua peringkat	**Semua**

maklumat. Terdapat peringkat dalam capaian maklumat dengan dikawal menggunakan akaun. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; f) Sesi yang tidak aktif perlu ditamatkan mengikut tempoh masa yang ditetapkan. g) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan h) Akaun pengguna boleh dibekukan dan ditamatkan atas sebab-sebab berikut:- a. Bertukar bidang tugas kerja; b. Bertukar ke agensi lain; c. Bersara; d. Digantung perkhidmatan ; atau e. Ditamatkan perkhidmatan	

8.6	**Pengurusan Kapasiti (*Capacity Management*)**
Objektif; Memastikan kemudahan kapasiti pemprosesan maklumat, sumber manusia, pejabat dan kemudahan lain yang diperlukan bagi minimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
Pengurusan kapasiti perlu dilaksanakan sebelum sistem dibangun dan dilaksanakan dengan mengambilkira keperluan 10 tahun. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Sumber yang diperlukan bagi sesuatu operasi seperti perkakasan, kemudahan, sumber manusia dan sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan b) Keperluan sumber ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	**Pentadbir Sistem Aplikasi,** **ICTSO**

8.7	**Perlidungan Terhadap Perisian *Malware* (*Protection Against Malware*)**
Objektif:	

Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya.	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Memasang sistem keselamatan seperti *anti virus* dan perisian keselamatan rangkaian untuk mengesan serangan siber dan mengesan aktiviti yang tidak diingini; b) Menggunakan 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*; d) Mengemas kini pattern *anti virus* yang terkini; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan h) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan *virus*.	**Semua**

8.8	**Pengurusan Kelemahan Teknikal (*Management Of Technical Vulnerabilities*)**
Objektif: Pengurusan kelemahan teknikal dalam keselamatan maklumat merujuk kepada proses mengenal pasti, menilai, dan mengurangkan kelemahan teknikal dalam sistem komputer, rangkaian dan aplikasi. Kelemahan Teknikal ialah kelemahan atau kecacatan dalam reka bentuk, pelaksanaan atau konfigurasi sistem yang boleh dieksploitasi oleh penyerang untuk mendapatkan akses tanpa kebenaran atau menyebabkan kemudaratan.	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut:- a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	**ICTSO dan Pentadbir Sistem Aplikasi**

8.9	**Pengurusan Konfigurasi (*Configuration Management*)**

Objektif:
Memastikan perkakasan, perisian, sistem aplikasi dan rangkaian berfungsi berdasarkan kawalan tetapan yang sepatutnya dan melindungi peranti daripada sebarang perubahan yang tidak dibenarkan atau pindaan yang tidak betul.

Dalam melaksanakan proses pengurusan konfigurasi untuk meminimumkan risiko keselamatan maklumat:- a) Memastikan bilangan pengguna yang mempunyai keistimewaan pentadbir (*administrator privilege*) pada tahap minimum; b) Melumpuhkan (*disable*) sebarang identiti yang tidak digunakan atau tidak diperlukan; c) Memantau dengan teliti capaian kepada program penyelenggaraan, aplikasi utiliti dan tetapan dalaman; d) Memastikan jam disegerakkan (*synchronised*) bagi tujuan jejak (*log*) konfigurasi dengan betul dan membantu dalam sebarang siasatan di masa hadapan; e) Menukar sebarang kata laluan atau tetapan keselamatan asal (*default*) yang dibekalkan dengan mana-mana peranti, perkhidmatan atau aplikasi; f) Melaksanakan log keluar secara automatik untuk mana-mana peranti, sistem atau aplikasi yang telah dibiarkan tidak aktif (*dormant*) dalam suatu tempoh masa tertentu; g) Memastikan semua keperluan pelesenan telah dipenuhi; h) Menguji setiap konfigurasi yang diperbaharui di dalam persekitaran penerimaan sebelum digunapakai dalam persekitaran sebenar apabila menaiktaraf aplikasi; i) Menjaga kerahsiaan konfigurasi; j) Pengguna tidak dibenarkan membuat sebarang pertukaran kepada konfigurasi yang telah ditetapkan; k) Pengguna tidak boleh mengubah konfigurasi alamat *IP* daripada alamat *IP* yang asal; l) Apabila bencana berlaku, sebelum konfigurasi baharu dibuat, sandaran (*backup*) hendaklah dibuat terlebih dahulu; m) Penyelenggaraan ke atas konfigurasi dilakukan dari masa ke semasa.	**ICTSO,** **Pentadbir Sistem Aplikasi,** **Seksyen Operasi dan Teknikal**

8.10	**Pemadaman Maklumat (*Information Deletion*)**

Objektif:

Pemadaman maklumat dalam keselamatan maklumat merujuk kepada proses mengalih keluar atau memusnahkan data dengan selamat daripada sistem komputer atau peranti storan. Ini termasuk pemadaman fail, *folder* dan keseluruhan *partition* atau cakera keras. Matlamatnya adalah untuk memastikan bahawa maklumat sensitif atau sulit tidak boleh dipulihkan oleh individu yang tidak dibenarkan dan untuk mengelakkan pelanggaran data.

Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut:- a) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat; b) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu dan dihapuskan dengan teratur dan selamat. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MBSA. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan dilakukan; b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; c) Peralatan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu 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; g) Pelupusan peralatan ICT hendaklah dilakukan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan h) Peralatan ICT hendaklah di *format* atau diubah kepada keadaan asal *(set to factory setting)* sebelum dilupuskan.	**Semua**

Semua kakitangan adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:- a) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman *CPU* seperti *RAM, hard disk, motherboard, modem* dan sebagainya; b) Menyimpan dan memindahkan perkakasan luaran komputer seperti *AVR, speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di MBSA; c) Memindah keluar dari MBSA mana-mana peralatan ICT yang hendak dilupuskan; d) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab MBSA; dan e) Semua kakitangan bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan; dan f) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana *Arahan Keselamatan* dan *Tatacara Jabatan Arkib Negara*.	

8.11	**Penyamaran Data (*Data Masking*)**
Objektif: Bagi membataskan keterdedahan data sensitif (sebarang data yang boleh dianggap sebagai maklumat pengenalan peribadi (*Personal Identification Information* atau PII) dan mematuhi garis panduan, peraturan dan keperluan kontrak.	
Dalam mempertimbangkan penyamaran data, perkara yang perlu diambil perhatian adalah:- a. Tahap penyamaran dan/atau penyamaran yang diperlukan, berbanding dengan sifat data; b. Cara data yang ditutup dicapai; c. Sebarang perjanjian yang menyekat penggunaan data untuk disembunyikan; d. Memastikan data yang ditutup diasingkan daripada	**ICTSO,** **Pentadbir Sistem ICT**

mana-mana jenis data lain untuk mengelakkan subjek data dikenal pasti dengan mudah; e. Membuat jejak log apabila data diterima dan bagaimana ia telah diberikan kepada mana-mana sumber dalaman atau luaran. Strategi pendekatan yang disusun untuk menutup data: a. Direka bentuk untuk menyamarkan (*disguise*) tujuan sebenar PII melalui pemisahan iaitu menyembunyikan pautan (*link*) antara data mentah dan subjek. Ini perlu berhati-hati bagi memastikan tiada satu pun data yang menjejaskan subjek. b. Melaksanakan teknik penyamaran yang hanya mendedahkan jumlah minimum data kepada sesiapa sahaja yang menggunakannya; c. Mengelirukan (*obfuscating*) atau menyembunyikan (*hiding*) cebisan data tertentu berdasarkan permintaan dan hanya membenarkan pengguna tertentu sahaja membuat capaian kepada bahagian yang berkaitan dengan mereka. Antara pilihan teknik yang boleh digunakan adalah: a. Nama samaran (*pseudonymisation*); b. Tanpa nama (*anonymisation*); c. Penyulitan berasaskan kunci (*key-based encryption*); d. Membatalkan (*voiding*) atau memadam aksara dalam set data; e. Mengubah (*varying*) nombor dan tarikh; f. Menggantikan nilai merentas data (*replacing values across the data*); g. Penyekat nilai berasaskan *hash* (*hash-based value masking*).	

8.12	**Pencegahan Kebocoran Data** ***(Data Leakage Prevention)***

Objektif:

Mengesan dan menghalang pendedahan dan pengekstrakan maklumat yang tidak dibenarkan oleh individu atau sistem.

Kebocoran data sukar untuk dihapuskan sepenuhnya. Walau bagaimanapun, untuk meminimumkan risiko yang unik untuk operasi mereka, organisasi harus: a) Memastikan e-mel atau data yang diterima adalah daripada organisasi yang sah; b) Memantau dengan teliti saluran data yang diketahui yang banyak digunakan dan terdedah kepada kebocoran (cth. 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 pemindahan data dilaksanakan; e) Semua klasifikasi maklumat/dokumen yang disampaikan melalui e-mel rasmi dan sebagainya perlu disediakan dalam bentuk fail kepilan (*attachment*) dan disulitkan (*encrypted*) sebelum dihantar; f) Pertimbangkan untuk mengurus atau menghalang pengguna daripada mengambil tangkapan skrin atau mengambil gambar monitor yang memaparkan jenis data yang dilindungi; g) Sulitkan sandaran yang mengandungi maklumat sensitif; h) Memastikan perisian sistem pengoperasian dan antivirus sentiasa dikemaskini.	**ICTSO, Pentadbir Sistem Aplikasi**

8.13	**Sandaran Maklumat** ***(Information Backup)***

Objektif:

Membolehkan pemulihan daripada kehilangan data atau sistem.

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran (*backup*) hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Membuat sandaran (*backup*) keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b) Membuat sandaran (*backup*) ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan sandaran (*backup*) bergantung pada tahap kritikal maklumat; c) Menguji sistem sandaran (*backup*) dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d) Menyimpan sandaran data mengikut jadual dan; e) Merekod dan menyimpan sandaran (*backup*) di lokasi yang berlainan dan selamat. Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat:- a) Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b) Capaian untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja; c) Pergerakan media storan hendaklah direkodkan; d) Pengguna bertanggungjawab terhadap keselamatan	**Semua**

maklumat dalam storan mudah alih seperti *thumbdrive* atau *external harddisk*; e) Perkakasan sandaran (*backup*) hendaklah diletakkan di tempat yang terkawal. Storan dan peralatan sandaran (*backup*) hendaklah disimpan di lokasi yang berasingan dan tidak terbuka kepada umum atau mengikut keperluan. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; f) Mengadakan salinan atau sandaran (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data.	

8.14	**Kemudahan Pemprosesan Maklumat Yang Bertindih** ***(Redundancy Of Information Processing Facilities)***
Objektif: Memastikan operasi fasiliti pemprosesan maklumat dapat diteruskan	
Kemudahan pemprosesan maklumat perlu mempunyai *redundancy* yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan *redundancy* perlu diuji (*failover test*) keberkesanannya dari masa ke semasa.	**ICTSO,** **Pentadbir Sistem Aplikasi**

8.15	**Log** ***(Logging)***
Objektif: Keselamatan maklumat log masuk merujuk kepada log maklumat seperti log masuk dan log keluar pengguna, capaian fail, sambungan rangkaian dan peristiwa sistem. Tujuan log adalah untuk merekod peristiwa, menghasilkan bukti, memastikan integriti maklumat log, menghalang akses yang tidak dibenarkan, mengenal pasti ancaman keselamatan maklumat yang boleh menyebabkan insiden keselamatan maklumat, dan menyokong penyiasatannya.	

Pentadbir Sistem Aplikasi hendaklah melaksanakan perkara-perkara berikut:- a) Mengadakan sistem log untuk merekod semua aktiviti harian pengguna; b) Menyemak dan meneliti sistem log untuk 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 Aplikasi hendaklah melaporkan kepada ICTSO dan CIO. Bagi pemantauan log perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala; c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MBSA atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	**Pentadbir Sistem Aplikasi**

8.16	**Aktiviti Pemantauan** ***(Monitoring Activities)***

Objektif:

Aktiviti pemantauan dalam keselamatan maklumat merujuk kepada proses berterusan memantau dan menganalisis sistem dan aktiviti rangkaian untuk mengenal pasti dan bertindak balas terhadap potensi ancaman dan kelemahan keselamatan.

Pentadbir Sistem mestilah bertanggungjawab mengesan, merekod dan menganalisis perkara-perkara berikut : a) Sebarang percubaan pencerobohan kepada sistem ICT MBSA; b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*deniel of service*), spam, pemalsuan (*forgery phising*), pencerobohan (*instrusion*), 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 Aplikasi.	**Pentadbir Sistem Aplikasi**

8.17	**Penyegerakan Jam** ***(Clock Synchronization)***
Objektif: Penyegerakan jam dalam keselamatan maklumat merujuk kepada proses memastikan bahawa jam pada sistem yang berbeza dan peranti yang berada di dalam rangkaian adalah tepat dan selari antara satu sama lain.	
Jam (masa) sistem harus disegerakkan dengan servis NTP ataupun GPS yang boleh dipercayai bagi memastikan log sistem tepat.	**Pengarah DTM, ICTSO**

8.18	**Keistimewaan Penggunaan Utiliti Program** ***(Use Of Privileged Utility Programs)***

Objektif:

Memastikan penggunaan program utiliti tidak membahayakan sistem dan kawalan aplikasi untuk keselamatan maklumat.

Penggunaan program utiliti dikawal ketat dan dihadkan serta perlu mematuhi perkara berikut: a) Hanya program atau perisian khas utiliti yang selamat sahaja digunakan; dan b) Penggunaan sistem utiliti perlulah dikawal dan dihadkan kepada pegawai yang dibenarkan saja.	**Pentadbir Sistem Aplikasi**

8.19	**Pemasangan Perisian Pada Sistem Operasi** ***(Installation Of Software On Operational Systems)***

Objektif:

Menjamin integriti sistem operasi dan mencegah penyalahgunaan kelemahan teknikal.

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

d) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan serta membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem Aplikasi; e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f) Pengguna mesti memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;	

h) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem Aplikasi atau Juruteknik untuk di baik pulih;

i) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (*UPS*);

j) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;

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

l) Peralatan ICT yang hendak dibawa keluar dari premis MBSA, perlulah mendapat kelulusan Pentadbir Sistem Aplikasi dan direkodkan bagi tujuan pemantauan;

m) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;

n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem Aplikasi;

p) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

q) Konfigurasi alamat *IP* tidak dibenarkan diubah daripada alamat *IP* yang asal;

r) Pengguna dilarang sama sekali mengubah kata laluan

bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Sistem Aplikasi / Juruteknik. Kata laluan bagi pentadbir (*administrator password*) adalah terhad untuk pengetahuan pentadbir sistem sahaja. Selain itu, kata laluan ini juga perlu dicipta berdasarkan saranan polisi umum bagi kata laluan agar ianya kukuh dan tidak mudah diketahui oleh pihak lain. Kata laluan ini juga hendaklah diubah secara berkala bagi mengelakkan kebocoran yang tidak diingini; s) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; t) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dimatikan apabila meninggalkan pejabat; u) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; v) Memastikan soket dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya; dan w) Memastikan setiap pemasangan aplikasi ataupun perisian hendaklah direkodkan, dan aplikasi ataupun perisian harus diuji dan dikemaskini sebelum dipasang dalam sistem *live* (*production*).	

8.20	**Keselamatan Rangkaian** ***(Networks Security)***

Objektif:

Memastikan maklumat dalam rangkaian dilindungi.

8.20.1	**Kawalan Infrastruktur Rangkaian**

Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara bagi menangani ancaman ke atas rangkaian yang perlu dipatuhi adalah seperti berikut:- a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d) Semua peralatan mestilah mengikut spesifikasi yang ditetapkan semasa pemasangan dan konfigurasi; e) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Sistem Aplikasi; f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan MBSA; g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h) Memasang perisian keselamatan rangkaian bagi mengesan sebarang cubaan menceroboh dan serangan siber yang boleh mengancam sistem dan maklumat MBSA; i) Sebarang penyambungan rangkaian yang bukan di bawah kawalan MBSA adalah tidak dibenarkan; j) Semua pengguna hanya dibenarkan menggunakan rangkaian MBSA sahaja dan penggunaan modem adalah dilarang sama sekali; dan k) Kemudahan bagi *wireless LAN* perlu dipastikan kawalan	**Pengarah DTM dan** **Ketua Seksyen Operasi & Teknikal**

keselamatan.	

8.21	**Keselamatan Perkhidmatan Rangkaian** ***(Security Of Network Services)***

Objektif:

Memastikan keselamatan dalam penggunaan perkhidmatan rangkaian; seperti e-mel, web, pemindahan fail dan perkhidmatan pangkalan data. Perkhidmatan ini sering disasarkan oleh penyerang kerana ia adalah kritikal kepada fungsi sesebuah organisasi dan lazimnya ia adalah titik masuk untuk penyerang mendapat akses kepada rangkaian.

Pengurusan bagi semua perkhidmatan rangkaian (*in house* atau *outsource*) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian. Pelaksanaan perkara-perkara berikut adalah perlu iaitu:- a) Pengurusan selamat perkhidmatan maklumat; b) Pemantauan perkhidmatan rangkaian; c) Penyelenggaraan konfigurasi Firewall, perisian keselamatan rangkaian, terutamanya peraturan ataupun '*Signatures'* perlu dibuat dari masa ke semasa.	**Pengarah DTM, Pentadbir Rangkaian**

8.22	**Pengasingan Rangkaian** ***(Segregation Of Networks)***

Objektif:

Memisahkan rangkaian dalam sempadan keselamatan dan mengawal trafik berdasarkan keperluan semasa.

Pengasingan rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian MBSA.	**Pengarah DTM dan** **Ketua Seksyen Operasi & Teknikal**

8.23	**Tapisan Laman Web** ***(Web Filtering)***

Objektif:

Menghapuskan risiko keselamatan seperti jangkitan perisian hasad (*malware*) yang mungkin timbul akibat capaian kepada laman web luaran dengan kandungan berniat jahat atau laman web yang tidak dibenarkan.

Organisasi meletakkan kawalan capaian dan langkah-langkah sekatan berikut:- a) Menyekat alamat IP atau domain laman web yang dikenal pasti sebagai berbahaya. Sebagai contoh, sesetengah pelungsur (*browser*) dan alat laman hasad (*anti-malware tools*) dilakukan secara automatik; b) Menentukan jenis-jenis laman web yang tidak boleh dicapai oleh kakitangan iaitu: a. Laman web dengan fungsi muat naik maklumat. Capaian hendaklah tertakluk kepada kebenaran dan hanya boleh diberikan atas sebab yang sah. b. Laman web yang diketahui atau disyaki mengandungi bahan berniat jahat, seperti laman web dengan kandungan perisian hasad (*malware*). c. Pelayan perintah dan kawalan (*command and control servers*). d. Laman web berniat jahat yang diperoleh daripada Risikan Ancaman (*Threat Intelligence*) (Kawalan 5.7). e. Laman web yang mengedarkan kandungan dan bahan yang menyalahi undang-undang. c) Menyemak dan mengemaskini kawalan dan peraturan pada selang masa yang tetap. Teknik penapisan web: a) Heuristik b) Tandatangan c) Senarai laman web yang dilarang dan boleh diterima d) Konfigurasi domain	**Pengarah DTM dan Ketua Seksyen Operasi & Teknikal**

8.24	**Penggunaan Kriptografi** ***(Use Of Cryptography)***

Objektif:

Memastikan penggunaan kriptografi adalah betul dan berkesan untuk melindungi kerahsiaan, ketulenan atau integriti maklumat mengikut keperluan.

8.24.1	**Enkripsi**	
Proses enkripsi (*encryption*) perlu dilaksanakan bagi melindungi kerahsiaan maklumat kritikal atau sensitif berdasarkan keperluan, penilaian risiko dan selaras dengan peraturan Majlis.		**Semua**

8.24.2	**Tandatangan Digital**	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya yang berurusan dengan transaksi maklumat kritikal atau sensitif atau maklumat rahsia rasmi secara elektronik.		**Semua**

8.25	**Kitaran Hidup Pembangunan Yang Selamat** ***(Secure Development Life Cycle)***

Objektif:

Memastikan keselamatan maklumat direka dan dilaksanakan dalam kitar hayat pembangunan yang selamat bagi perisian dan sistem.

Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Keselamatan persekitaran pembangunan; b) Keselamatan pangkalan data; 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 penyumberluaran (*outsource*), pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan	**Pengarah DTM, ICTSO, Pentadbir Sistem Aplikasi**

8.26	**Keperluan Keselamatan Aplikasi** ***(Application Security Requirements)***

Objektif:

Keperluan keselamatan aplikasi dalam keselamatan maklumat merujuk kepada satu set garis panduan dan piawaian yang digunapakai oleh MBSA untuk memastikan bahawa aplikasi perisian mereka selamat dan bebas daripada kelemahan.

Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada. Keperluan keselamatan maklumat bagi pembangunan sistem baharu dan penambahbaikan sistem hendaklah mematuhi perkara-perkara berikut: a) Memastikan pembekal yang dipertanggungjawabkan mempunyai kelayakan dalam bidang berkaitan dan pembekal yang berdaftar dengan Kementerian Kewangan; b) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna; c) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan; d) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; e) Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data. f) Pelaksanaan aktiviti keselamatan ICT seperti *Penetration Testing* dan sebagainya boleh dilakukan terhadap sistem-sistem utama.	**Pengarah DTM, ICTSO, Pentadbir Sistem Aplikasi**

8.27	***Prinsip Senibina Sistem dan Kejuruteraan Yang Selamat*** ***(Secure System Architecture and Engineering Principles)***

Objektif:

Memastikan sistem maklumat direka, dilaksanakan, dan beroperasi dengan selamat dalam kitar hayat pembangunan. Membolehkan organisasi mengekalkan keselamatan sistem maklumat sepanjang sistem di dalam SDLC.

Spesifikasi reka bentuk perlu memasukkan keperluan keselamatan sistem maklumat. Sekiranya sesuatu *off-the-shelves* produk diperolehi, pembekal perlu dimaklumkan berkenaan keperluan keselamatan. Organisasi harus menekankan keselamatan ke atas semua lapisan sistem maklumat, termasuk proses perkhidmatan, aplikasi dan seni bina data. Prinsip kejuruteraan yang selamat harus digunakan untuk semua aktiviti yang berkaitan dengan sistem maklumat dan harus tertakluk kepada semakan dan kemas kini yang kerap dengan mengambil kira ancaman dan corak serangan yang muncul. Prinsip ini juga digunakan untuk sistem maklumat yang dibangunkan secara dalaman mahupun sumber luar. Oleh itu, organisasi harus memastikan bahawa amalan dan piawaian penyedia perkhidmatan sumber luar mematuhi prinsip kejuruteraan organisasi. Beberapa langkah utama melaksanakan seni bina dan kejuruteraan sistem yang selamat dalam keselamatan maklumat: a) Menjalankan latihan pemodelan ancaman (*threat modelling*); b) Melaksanakan prinsip hak keistimewaan yang paling sedikit (*least privilege*); c) Menggunakan pertahanan secara mendalam;Menjalankan penilaian kerentanan (*vulnerabilities*) secara berkala; d) Menggunakan amalan pengekodan selamat; e) Merancang tindak balas insiden; f) Kekerapan memantau dan menyemak sistem.	**Pengarah DTM, ICTSO**

8.28	**Pengekodan Selamat** ***(Secure Coding)***

Objektif:

Pengekodan selamat merujuk kepada amalan menulis kod komputer yang selamat dan kurang terdedah kepada serangan. Ia melibatkan penggunaan teknik dan kaedah untuk menghalang kelemahan keselamatan daripada diperkenalkan ke dalam kod semasa proses pembangunan.

Ini termasuk amalan reka bentuk dan pengekodan yang meminimumkan risiko perisian biasa kelemahan seperti *Buffer Overflow, SQL Injection* dan cross-site scripting. Pengekodan selamat juga termasuk piawaian, garis panduan dan amalan terbaik. Selain itu, pengekodan selamat juga termasuk menguji dan menyemak kod untuk mengenal pasti dan membetulkan sebarang isu keselamatan sebelum penggunaan

Organisasi harus memastikan prinsip pengekodan selamat dipatuhi untuk kedua-dua produk perisian yang diperoleh daripada pihak luar dan kepada komponen perisian sumber terbuka sama ada projek pengekodan baharu dan juga operasi penggunaan semula perisian meliputi aktiviti pembangunan perisian dalaman dan pemindahan produk atau perkhidmatan perisian organisasi kepada pihak ketiga. Prasyarat pengekodan selamat, organisasi harus mematuhi perkara berikut:- a) Menentukan jangkaan keselamatan yang disesuaikan dengan keperluan mereka dan mewujudkan prinsip yang diluluskan untuk pengekodan perisian yang selamat yang akan digunakan untuk kedua-dua pembangunan perisian secara dalaman dan komponen perisian sumber luar; b) Mengesan dan mendokumentasikan amalan reka bentuk pengekodan yang paling lazim dan sejarah amalan pengekodan buruk serta kesilapan yang mengakibatkan kesan kepada keselamatan maklumat; c) Menyediakan dan mengkonfigurasi alat pembangunan (*development tools*) perisian untuk memastikan keselamatan semua kod yang diwujudkan; d) Mencapai pematuhan dengan panduan dan arahan yang disediakan oleh alat pembangunan (*development tools*) perisian; e) Menyemak, menyelenggara dan menggunakan alat pembangunan (*development tools*) dengan selamat seperti penyusun (*compilers*);	**Pengarah DTM, ICTSO**

Panduan keselamatan pengekodan selamat:

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 dipacu ujian (*test-driven development*) dan pengaturcaraan pasangan (*pair programming*);

c) Penggunaan kaedah pengaturcaraan berstruktur (*structured programming methods*);

d) Dokumentasi kod yang betul dan penyingkiran kecacatan kod (*removal of code defects*);

e) Larangan ke atas penggunaan kaedah pengekodan perisian yang tidak selamat seperti sampel kod yang tidak diluluskan atau kata laluan berkod keras (*hardcoded passwords*);

f) Ujian keselamatan dilakukan semasa dan selepas pembangunan mengikut **Kawalan 8.29.**

Sebelum meletakkan perisian itu dalam penggunaan sebenar dalam persekitaran aplikasi langsung, organisasi harus mempertimbangkan perkara berikut:

a) Apakah permukaan serangan?

b) Adakah prinsip keistimewaan yang paling sedikit diikuti?

c) Melaksanakan analisis ke atas kesilapan pengaturcaraan yang paling lazim berlaku dan mendokumentasikan bahawa risiko ini telah dihapuskan.

Selepas Kod Digunakan dalam Persekitaran Pengeluaran:

a) Pengemaskinian harus digunakan dengan cara yang selamat;

b) Kerentanan keselamatan (*security vulnerabilities*) yang dilaporkan selaras dengan **Kawalan 8.8** harus ditangani;

c) Serangan yang disyaki terhadap sistem maklumat dan ralat hendaklah direkodkan dan rekod ini hendaklah disemak secara berkala supaya perubahan yang sesuai kepada kod boleh dibuat;

d) Capaian tanpa kebenaran kepada, penggunaan atau perubahan kepada kod sumber harus dihalang melalui mekanisme seperti alat pengurusan (*management tools*).

Apabila organisasi menggunakan alat (*tools*) luaran, perkara berikut harus diambil kira:

a) Perpustakaan luaran (*external libraries*) hendaklah dipantau dan dikemas kini pada selang masa yang tetap berdasarkan kitaran keluarannya;

b) Komponen perisian hendaklah disemak, dipilih dan dibenarkan dengan teliti terutamanya komponen kriptografi dan pengesahan;

c) Pelesenan komponen luaran dan memastikan keselamatannya;

d) Perisian harus dijejaki dan diselenggara. Ia mesti dipastikan datang dari sumber yang boleh dipercayai;

e) Sumber pembangunan harus tersedia untuk jangka masa panjang.

Organisasi harus memastikan bahawa kod berkaitan keselamatan digunakan apabila perlu dan tahan terhadap gangguan. Cadangan untuk kod berkaitan keselamatan:

a. Walaupun program yang dipasang melalui kod binari termasuk kod berkaitan keselamatan, ini terhad kepada data yang disimpan dalam aplikasi itu sendiri;

b. Konsep kod berkaitan keselamatan hanya berguna apabila kod dijalankan pada pelayan (*server*) yang tidak boleh diakses oleh pengguna dan ia diasingkan daripada proses yang menggunakannya dan datanya disimpan dengan selamat dalam pangkalan data lain. Sebagai contoh, anda boleh menjalankan kod yang ditafsirkan pada perkhidmatan awan dan capaian kepada kod boleh dihadkan kepada pentadbir khas (*privileged administrators*). Adalah disyorkan agar anda melindungi hak capaian ini melalui kaedah seperti keistimewaan pentadbir tepat pada masanya dan mekanisme pengesahan yang mantap;

c. Konfigurasi yang sesuai pada pelayan web harus dilaksanakan untuk menghalang akses tanpa kebenaran dan menyemak imbas direktori;

d. Apabila mereka bentuk kod aplikasi, anda harus bermula dengan andaian bahawa kod itu terdedah kepada serangan disebabkan oleh ralat pengekodan dan tindakan oleh pelaku

yang berniat jahat (*malicious actors*). Anda harus mereka bentuk aplikasi kritikal dengan cara yang tidak terdedah kepada kerosakan dalaman. Sebagai contoh, output yang dihasilkan oleh algoritma boleh disemak untuk memastikan ia mematuhi keperluan keselamatan sebelum ia boleh digunakan dalam aplikasi kritikal seperti aplikasi berkaitan kewangan; e. Organisasi harus merujuk kepada siri ISO/IEC 15408 untuk mendapatkan maklumat lanjut tentang penilaian keselamatan IT bagi ancaman keselamatan terhadap aplikasi web yang disebabkan oleh amalan pengekodan yang lemah seperti suntikan pangkalan data (*database injection*) dan serangan skrip merentas tapak (*cross-site scripting attacks*).	

8.29	**Ujian Keselamatan Dalam Pembangunan Dan Penerimaan** ***(Security Testing In Development And Acceptance)***
Objektif: Ujian keselamatan dalam pembangunan dan penerimaan ialah proses yang membantu mengenal pasti dan mengurangkan kelemahan keselamatan dalam aplikasi perisian sebelum ia digunakan. Ujian jenis ini biasanya dilakukan semasa fasa pembangunan dan penerimaan SDLC.	
Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut: 1. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; 2. Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat; dan 3. Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem; Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin keselamatan. Tiga (3) elemen yang harus diambil kira dalam proses ujian keselamatan: a. Fungsi keselamatan seperti Pengesahan Pengguna (Kawalan 8.5), Sekatan Capaian (Kawalan 8.3) dan Kriptografi (Kawalan 8.24);	**Pengarah DTM, ICTSO, Pentadbir Sistem Aplikasi**

b. Pengekodan Selamat (Kawalan 8.28); c. Konfigurasi Selamat (Kawalan 8.9, 8.20 dan 8.22). Ini mungkin meliputi *Firewall* dan sistem pengendalian. Kaedah ujian dalam pembangunan adalah: a. Ulasan kod; b. Ujian penembusan; c. Ujian fuzz. Kaedah ujian dalam penerimaan adalah: a. Ujian kefungsian; b. Ujian prestasi; c. Ujian keselamatan.	

8.30	**Pembangunan Sumber Luar** ***(Outsourced Development)***
Objektif: Membolehkan organisasi memastikan keperluan keselamatan maklumat yang ditetapkan dipatuhi apabila sistem dan pembangunan perisian disalurkan kepada pembekal luar. Pembangunan sumber luar dalam keselamatan maklumat merujuk kepada amalan mengupah pihak ketiga, syarikat atau individu untuk membangunkan perisian atau melaksanakan tugas lain yang berkaitan dengan IT. Ini boleh termasuk tugasan seperti pembangunan perisian, ujian, penyelenggaraan dan sokongan.	
Pembangunan aplikasi secara *outsource* perlu diselia dan dipantau oleh pegawai yang dipertanggungjawabkan. Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik Majlis. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Perkiraan pelesenan, kod sumber ialah **HAK MILIK MBSA** dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara *outsource*; b. Bagi semua perkhidmatan sumber luaran, perisian sebagai	**JDTM dan Pentadbir Sistem Aplikasi**

satu perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori "Pembekal hendaklah membenar MBSA mencapai kod sumber dan melaksanakan pengolahan risiko; c. Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik; d. Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem; e. Pemindahan teknologi (*Transfer Of Technology*) mesti dilaksanakan oleh kontraktor kepada pengguna; f. Perjanjian termasuk perjanjian pelesenan merangkumi pemilikan ke atas kod dan hak harta intelek g. Mengenakan keperluan kontrak yang sesuai untuk reka bentuk dan pengekodan selamat (Kawalan 8.25 dan 8.29); h. Menyediakan model ancaman (*threat model*) untuk diguna pakai oleh pembangun pihak ketiga. i. Menjalankan prosedur ujian penerimaan untuk memastikan kualiti dan ketepatan kerja yang dihantar. j. Bukti bahawa keupayaan privasi dan keselamatan yang diperlukan secara minima telah dicapai. Ini boleh dicapai melalui laporan jaminan. k. Menyimpan bukti tentang cara ujian yang mencukupi telah dilakukan untuk melindungi sistem atau perisian IT yang dihantar daripada kandungan berniat jahat (*malicious content*). l. Menyimpan bukti tentang sejauh mana ujian yang mencukupi telah dilaksanakan untuk melindungi daripada kelemahan yang dikenal pasti. m. Menyediakan perjanjian escrow yang meliputi kod sumber perisian. Sebagai contoh, ia mungkin menangani perkara yang akan berlaku jika pembekal luar keluar dari perniagaan. n. Perjanjian dengan pembekal harus melibatkan hak organisasi	

untuk melaksanakan audit ke atas proses dan kawalan pembangunan. o. Mewujudkan dan melaksanakan keperluan keselamatan untuk persekitaran pembangunan. p. Undang-undang, statut dan peraturan yang terpakai.	

8.31	**Pengasingan Persekitaran Pembangunan, Pengujian Dan Pengeluaran** ***(Separation Of Development, Test And Production Environments)***

Objektif:

Pengasingan persekitaran pembangunan, ujian dan pengeluaran dalam keselamatan maklumat merujuk kepada amalan mengekalkan persekitaran yang berasingan untuk fasa berbeza mengikut SDLC.

Dengan adanya pengasingan ini akan dapat membantu menghalang sebarang isu yang mungkin berlaku dalam pembangunan atau persekitaran pengujian daripada menjejaskan pengeluaran persekitaran. Ia juga membantu untuk menghalang sebarang capaian yang tidak dibenarkan, pengubahsuaian atau pemadaman secara tidak sengaja data pengeluaran dan konfigurasi.

Perkara-perkara yang perlu dipatuhi adalah seperti 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 agensi. Individu atau suatu kumpulan tertentu 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 sahaja; d. Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e. Menghalang sebarang peluang untuk membocorkan maklumat; f. Pengasingan dan pengendalian sistem pembangunan dan	**CIO,** **Pemilik Sistem dan** **Pentadbir Sistem Aplikasi**

pengeluaran dilakukan ke tahap yang mencukupi. Sebagai contoh, penggunaan persekitaran maya dan fizikal yang berasingan untuk pengeluaran boleh menjadi kaedah yang berkesan; g. Peraturan dan prosedur kebenaran yang sesuai hendaklah diwujudkan, didokumenkan dan digunakan untuk penggunaan perisian dalam persekitaran pengeluaran selepas melalui persekitaran pembangunan; h. Organisasi harus menyemak dan menguji perubahan yang dibuat pada aplikasi dan sistem pengeluaran dalam persekitaran ujian berasingan daripada persekitaran pengeluaran sebelum perubahan ini digunakan dalam persekitaran pengeluaran; i. Pengujian dalam persekitaran pengeluaran tidak boleh dibenarkan melainkan pengujian tersebut ditakrifkan dan diluluskan sebelum pengujian; j. Alat pembangunan (*development tools*) seperti penyusun (*compilers*) dan penyunting (*editors*) tidak boleh dicapai daripada persekitaran pengeluaran melainkan capaian ini benar-benar diperlukan; k. Untuk meminimumkan ralat, label pengenalan persekitaran yang betul hendaklah dipaparkan dengan jelas dalam menu; l. Aset maklumat sensitif tidak boleh dipindahkan ke dalam persekitaran pembangunan dan pengujian melainkan langkah keselamatan yang setara digunakan dalam sistem pembangunan dan sistem pengujian.	

8.32	**PENGURUSAN PERUBAHAN** ***(CHANGE MANAGEMENT)***

Objektif:

Pengurusan perubahan dalam keselamatan maklumat merujuk kepada proses mengurus dan mengawal perubahan kepada sistem maklumat, aplikasi dan infrastruktur. Ini termasuk
perubahan pada perkakasan, perisian dan konfigurasi rangkaian.

8.32.1	Kawalan Perubahan Perkakasan ICT	
Perubahan yang melibatkan perkakasan rangkaian dan komunikasi, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah dikemukakan oleh pemilik sistem atau pentadbir rangkaian dan komunikasi dan mendapat kebenaran daripada pegawai yang diberi kuasa; dan Sebarang perubahan komponen sistem ICT hendaklah mematuhi keperluan yang ditetapkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Pengubahsuaian yang melibatkan perkakasan rangkaian dan komunikasi, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen 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; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak	**Semua**
8.32.2	**Kawalan Perubahan Sistem ICT**	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perubahan dan pengubahsuaian ke atas sistem perisian aplikasi dan maklumat hendaklah dikawal, diuji, direkodkan dan disahkan melalui prosedur yang ditetapkan sebelum diguna pakai; b. Pengujian terhadap perubahan dan pengubahsuaian ke atas sistem perisian aplikasi dan maklumat hendaklah dilaksanakan dalam persekitaran yang berasingan samada daripada produksi atau pembangunan; c. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu	**Semua**

perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; d. Mengawal perubahan dan /atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; e. Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan f. Menghalang sebarang peluang untuk membocorkan maklumat.	

8.33	**Maklumat Ujian** ***(Test Information)***

Objektif:

Maklumat ujian dalam keselamatan maklumat merujuk kepada data dan maklumat yang digunakan untuk melaksanakan keselamatan ujian ke atas aplikasi perisian, prosedur, sistem dan infrastruktur. Ia termasuk kes ujian, ujian data, skrip ujian dan maklumat lain yang digunakan untuk menilai keselamatan sistem yang diuji.

Melindungi dan mengekalkan kerahsiaan maklumat yang digunakan dalam persekitaran pengujian serta membuat pemilihan dan penggunaan maklumat pengujian yang akan menghasilkan keputusan yang boleh dipercayai.

Data pengujian sistem perlu dipilih dengan teliti, dilindungi dan terkawal. Penggunaan data sebenar (operational data) yang melibatkan data personel atau data sensitif pada persekitaran pengujian perlu dielakkan. Jika data personel atau data sensitif digunakan untuk tujuan pengujian, kandungan sensitif perlu ditapis atau diubahsuai sebelum digunakan. Organisasi hendaklah mematuhi perkara berikut dalam melindungi maklumat sensitif, termasuk data peribadi, dalam pembangunan dan persekitaran pengujian: a. Kawalan capaian yang digunakan dalam persekitaran dunia sebenar juga harus dilaksanakan dalam persekitaran pengujian; b. Mewujudkan dan melaksanakan prosedur kebenaran yang berasingan untuk menyalin maklumat sebenar ke dalam persekitaran pengujian;	**Pengarah DTM, ICTSO**

c. Merekodkan semua aktiviti yang berkaitan dengan penyalinan dan penggunaan maklumat sensitif dalam persekitaran pengujian untuk mengekalkan jejak audit; d. Melaksanakan kawalan yang sesuai seperti penyamaran data (*data masking*) atau penyingkiran data bagi tujuan perlindungan jika maklumat sensitif akan digunakan dalam persekitaran pengujian; e. Mengalih keluar maklumat yang digunakan dalam persekitaran ujian secara selamat dan kekal setelah pengujian selesai untuk menghapuskan risiko capaian tanpa kebenaran.	

8.34	**Perlindungan Sistem Maklumat Semasa Pengujian Audit** ***(Protection Of Information Systems During Audit Testing)***
Objektif: Perlindungan sistem maklumat semasa ujian audit dalam keselamatan maklumat merujuk kepada langkah dan prosedur yang disediakan untuk melindungi sistem maklumat ketika ia diuji semasa audit.	
Keperluan dan aktiviti audit yang melibatkan pengujian sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses kelancaran sistem. Untuk melindungi sistem semasa pengujian audit, organisasi boleh melaksanakan beberapa langkah: a. Penggunaan akaun pengujian: gunakan akaun pengujian dan bukannya akaun sebenar untuk mengakses sistem semasa ujian. Ini boleh membantu untuk mengelakkan perubahan yang tidak disengajakan atau tidak dibenarkan pada sistem; b. Penggunaan data pengujian: gunakan data pengujian dan bukannya data sebenar untuk melaksanakan pengujian. Ini boleh membantu untuk melindungi data sensitif atau data sulit daripada dikompromi; c. Pengasingan persekitaran ujian: asingkan persekitaran ujian daripada persekitaran pengeluaran untuk mencegah gangguan atau kerosakan kepada persekitaran pengeluaran; d. Sandaran data (*data backup*): lakukan sandaran sistem (*system*	**Pengarah DTM, ICTSO**

backup) sebelum pengujian - Perlu sekiranya sistem perlu dipulihkan apabila berlaku kejadian yang tidak dijangka; e. Pemantauan: memantau sistem semasa pengujian untuk mengesan sebarang isu atau masalah yang mungkin berlaku; f. Pelan pengujian: mempunyai pelan pengujian terperinci dan berkomunikasi dengan pihak yang berkaitan seperti pentadbir sistem dan pihak berkepentingan lain. Keperluan khusus yang harus dipertimbangkan oleh organisasi: a. Pengurusan dan juruaudit harus bersetuju mengenai capaian kepada sistem dan aset maklumat; b. Perjanjian mengenai skop pengujian audit teknikal yang akan dilaksanakan; c. Organisasi hanya boleh menyediakan capaian baca sahaja (*read-only*) kepada maklumat dan perisian. Sekiranya tidak mungkin untuk menggunakan teknik baca sahaja, pentadbir yang mempunyai hak capaian yang diperlukan boleh mendapatkan capaian kepada sistem atau data bagi pihak juruaudit; d. Jika permintaan capaian dibenarkan, organisasi hendaklah terlebih dahulu mengesahkan bahawa peranti yang digunakan untuk mencapai sistem memenuhi keperluan keselamatan sebelum mereka menyediakan capaian; e. Capaian hanya perlu disediakan untuk salinan terpencil fail (*isolated copies of files*) yang diekstrak daripada sistem. Salinan ini harus dipadamkan secara kekal setelah audit selesai melainkan terdapat keperluan untuk mengekalkan fail tersebut. Jika capaian baca sahaja boleh dilakukan, kawalan ini tidak terpakai; f. Permintaan oleh juruaudit untuk melaksanakan pemprosesan khas seperti menggunakan alat audit (*audit tools*) perlu dipersetujui oleh pihak pengurusan; g. Jika audit menyebabkan risiko yang menjejaskan ketersediaan sistem, audit hendaklah dijalankan di luar waktu operasi perkhidmatan untuk mengekalkan ketersediaan maklumat; h. Permintaan capaian yang dibuat untuk audit hendaklah direkodkan untuk jejak audit.	

GLOSARI	
Antivirus	Perisian yang mengimbas *virus* pada media storan seperti disket, cakera padat, pita magnetik, optical disk, flash disk, CDROM, thumb drive untuk sebarang kemungkinan adanya *virus*.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Sandaran atau proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur. Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial Of Service	Halangan pemberian perkhidmatan
Downloading	Aktiviti muat-turun sesuatu perisian
DTM	Jabatan Digital Dan Teknologi Maklumat
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya 1tidak difahami oleh orang lain kecuali penerima yang sah
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*)
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas
Hub	Hab (hub) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain
ICT	Information and Communication Technology (Teknologi Maklumat dan Komunikasi)
ICTSO	ICT Security Officer Pegawai yang bertanggungjawab terhadap keselamatan sistem

	computer
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based* IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer
Logout	*Logout* komputer Keluar daripada sesuatu sistem atau aplikasi komputer
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan *virus*, *trojan horse, worm, spyware* dan sebagainya
MODEM	MOdulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan
Public-Key Infrastructure (PKI)	Infrastruktur Kekunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi

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