# PENGENALAN

MAJLIS DAERAH MARANG

## 1.0 PENGENALAN

Garis panduan ini bertujuan untuk memberikan panduan tentang penggunaan peralatan ICT serta tanggungjawab dan peranan setiap pengguna semasa mengguna pakai peralatan tersebut berdasarkan kepada Dasar Keselamatan ICT.

## 2.0 TUJUAN

DKS MDM diwujudkan untuk memastikan pengurusan tadbir urus keselamatan siber bagi semua inisiatif digital MDM dipatuhi bagi meredakan kebimbangan mengenai masalah keselamatan maklumat.

## 3.0 OBJEKTIF

Objektif utama DKS MDM ialah seperti berikut:

(i) Memastikan kelancaran operasi pendigitalan MDM dan meminimumkan kerosakan atau kemusnahan disebabkan insiden keselamatan siber;
(ii) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem ICT daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan telekomunikasi;
(iii) Mencegah salah guna atau kecurian aset ICT dan siber Kerajaan;
(iv) Meminimumkan kos penyelenggaraan aset ICT akibat ancaman, godaman dan penyalahgunaan;
(v) Memperkemaskan pengurusan keselamatan siber MDM; dan
(i) Menghindari tindakan penggodaman ruang siber yang dituju kepada sistem ICT atau laman web rasmi MDM.

# PENGURUSAN ASET

MAJLIS DAERAH MARANG

## PENGURUSAN ASET

| **Akauntabiliti Aset**<br><br>**Objektif:** Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MDM/ Jabatan/ Agensi di bawah MDM. | |
|---|---|
| **Aset ICT** | **Tanggungjawab** |
| Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh Pengguna masing-masing.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Memastikan semua aset ICT perolehan secara pembelian dikenal pasti dan maklumat aset direkodkan serta dikemaskini dari semasa ke semasa ke dalam sistem pengurusan aset berdasarkan pekeliling yang sedang berkuatkuasa;<br><br>(b) Memastikan semua aset perolehan secara sewaan dikenal pasti dan maklumat aset direkodkan serta dikemaskini dari semasa ke semasa;<br><br>(c) Memastikan semua aset ICT diuruskan oleh Pendaftar Peralatan ICT dan dikendalikan oleh Pengguna yang dibenarkan sahaja;<br><br>(d) Memastikan semua Pengguna mengesahkan penempatan aset ICT yang ditempatkan;<br><br>(e) Peraturan bagi pengendalian aset ICT hendaklah dipatuhi dan dilaksanakan;<br><br>(f) Setiap Pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan<br><br>(g) Memastikan semua aset ICT diagihkan kepada Pengguna | Pegawai Aset, Pentadbir Peralatan ICT MDM/ Jabatan/ Agensi di bawah MDM dan Pengguna |

| | |
|---|---|
| mengikut piawaian dan garis panduan yang ditetapkan. | |
| **Pengelasan, Pengendalian dan Keselamatan Maklumat**<br><br>**Objektif:** Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian. | |
| **Pengelasan Maklumat** | **Tanggungjawab** |
| Maklumat hendaklah dikelaskan sewajarnya oleh pegawai yang diberi kuasa mengikut Arahan Keselamatan Kerajaan yang sedang berkuatkuasa.<br><br>Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan dalam Arahan Keselamatan Kerajaan yang sedang berkuatkuasa seperti berikut:<br><br>(a) Rahsia Besar;<br>(b) Rahsia;<br>(c) Sulit; atau<br>(d) Terhad. | Pegawai Pengelas |
| **Pelabelan Maklumat** | **Tanggungjawab** |
| Maklumat hendaklah dilabelkan sewajarnya.<br><br>Penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan Kerajaan yang sedang berkuatkuasa seperti berikut:<br><br>(a) Rahsia Besar; | Pengguna |

| | |
|---|---|
| (b) Rahsia;<br>(c) Sulit; atau<br>(d) Terhad | |
| **Pengendalian Maklumat** | **Tanggungjawab** |
| Aktiviti pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan hendaklah mengambil kira langkah-langkah keselamatan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;<br>(b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;<br>(c) Menentukan maklumat sedia untuk digunakan;<br>(d) Menjaga kerahsiaan kata laluan;<br>(e) Mematuhi *standard*, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;<br>(f) Memberi perhatian terutama semasa aktiviti pengendalian maklumat terperingkat;<br>(g) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum; dan<br>(h) Mewujudkan sandaran/ salinan pendua maklumat penting bagi mengurangkan risiko kehilangan dan kemusnahan serta memelihara kerahsiaan maklumat terperingkat. | Pengguna |

| Keselamatan Maklumat | Tanggungjawab |
|---|---|
| Keselamatan maklumat penting bagi perlindungan data- dalam-penggunaan, data-dalam-pergerakan, data-dalam- simpanan dan menghalang ketirisan data.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Maklumat terperingkat hanya boleh dilakukan penduaan dan penyalinan pada media storan oleh Pengguna yang dibenarkan sahaja;<br><br>(b) Menggunakan teknologi enkripsi dan lain-lain kaedah keselamatan yang bersesuaian ke atas maklumat terperingkat yang disediakan dan dihantar secara elektronik; dan<br><br>(c) Semua maklumat terperingkat hendaklah dihapuskan mengikut prosedur pelupusan semasa yang sedang berkuatkuasa. | Pengguna |
| **ICT Hijau Kerajaan (Government Green ICT)**<br><br>**Objektif:** Memastikan aset ICT mematuhi ciri-ciri ICT Hijau Kerajaan. | |
| **Pengurusan Aset ICT** | **Tanggungjawab** |
| Amalan penggunaan peralatan ICT ke arah ICT Hijau bagi mengurangkan penggunaan tenaga.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Memastikan perolehan aset ICT mengambil kira pematuhan elemen ICT Hijau Kerajaan; | PICT,<br>Pentadbir Peralatan ICT MDM/ Jabatan/ Agensi di bawah MDM |

| | |
|---|---|
| (b) Memastikan kerja-kerja seharian mengguna pakai prinsip pengurangan (reduce), penggunaan semula (reuse) dan kitar semula (recycle);<br><br>(c) Memastikan sistem pengurusan kuasa (power management) aset ICT diaktifkan; dan<br><br>(d) Memastikan peralatan ICT dilupuskan dan penggunaan semula alat ganti mengikut prosedur yang mengambil kira pemuliharaan alam sekitar. | dan<br>Pengguna |

# KAWALAN CAPAIAN AKSES

MAJLIS DAERAH MARANG

## KAWALAN CAPAIAN/ AKSES

**Dasar Kawalan Capaian/ Akses**

**Objektif:** Peraturan kawalan capaian hendaklah mengambil kira faktor **had** capaian dan **hak** capaian (authorization) ke atas data dan maklumat serta proses capaian maklumat.

| Keperluan Kawalan Capaian/ Akses | Tanggungjawab |
|---|---|
| Kawalan Capaian**/** Akses merupakan pendekatan untuk mengehadkan capaian sistem kepada Pengguna yang berdaftar.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Melaksanakan kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan Pengguna;<br>(b) Melaksanakan kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;<br>(c) Melaksanakan keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan<br>(d) Melaksanakan kawalan ke atas kemudahan pemprosesan maklumat. | Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT, Pentadbir Peralatan ICT MDM/ Jabatan/ Agensi di bawah MDM dan Pengguna |

| Pengurusan Capaian/ Akses Pengguna<br><br>**Objektif:** Mengawal capaian pengguna ke atas aset ICT MDM/ Jabatan/ Agensi di bawah MDM. | |
|---|---|
| **Akaun Pengguna** | **Tanggungjawab** |
| Setiap Pengguna adalah bertanggungjawab ke atas aset ICT yang digunakan. Akaun Pengguna diwujudkan bagi mengenalpasti Pengguna dan aktiviti yang dilakukan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Akaun yang diperuntukkan sahaja boleh digunakan;<br><br>(b) Akaun Pengguna mestilah unik;<br><br>(c) Pengguna bertanggungjawab sepenuhnya ke atas segala kegunaan melalui akaun dan kata laluannya;<br><br>(d) Akaun Pengguna akan dibeku atau ditamatkan atas sebab-sebab berikut:<br><br>i. Pengguna yang bercuti panjang dalam tempoh waktu melebihi 30 hari;<br>ii. Bertukar bidang tugas kerja;<br>iii. Bertukar ke agensi lain;<br>iv. Bersara; atau<br>v. Ditamatkan perkhidmatan.<br><br>(e) Sebarang perubahan tahap akses bagi Pengguna hendaklah mendapat kelulusan daripada Pemilik Sistem; dan<br><br>(f) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang. | Pemilik Sistem, Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT MDM/ Jabatan/ Agensi di bawah MDM dan Pengguna |

| Hak Capaian/ Akses | Tanggungjawab |
|---|---|
| Pengurusan dan pemantauan hak capaian terhadap akaun-akaun dan sistem aplikasi.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas; dan<br><br>(b) Hak capaian Pengguna diberi berdasarkan peranan dan tanggungjawab Pengguna. | Pemilik Sistem,<br>Pentadbir Sistem ICT,<br>Pentadbir Pusat Data Rangkaian dan Komunikasi ICT<br>MDM/ Jabatan/ Agensi di bawah MDM<br>dan<br>Pengguna |
| **Pengurusan Kata Laluan** | **Tanggungjawab** |
| Pengurusan kata laluan mestilah mematuhi amalan terbaik serta memastikan keselamatan kata laluan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;<br><br>(b) Kata laluan hendaklah ditukar apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;<br><br>(c) Kata laluan hendaklah sekurang-kurangnya dua belas (12) aksara dengan gabungan aksara, angka dan aksara khusus;<br><br>(d) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun; | Pentadbir Sistem ICT,<br>Pentadbir Pusat Data Rangkaian dan Komunikasi ICT<br>MDM/ Jabatan/ Agensi di bawah MDM<br>dan<br>Pengguna |

| | |
|---|---|
| (e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan apabila meninggalkan komputer melebihi 10 minit;<br>(f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;<br>(g) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;<br>(h) Kata laluan hendaklah ditukar dalam tempoh yang ditetapkan; dan<br>(i) Sistem aplikasi yang dibangunkan digalakkan mempunyai kemudahan menukar kata laluan oleh Pengguna. | |
| ***Clear Desk* dan *Clear Screen*** | **Tanggungjawab** |
| *Clear Desk* dan *Clear Screen* merupakan amalan yang digalakkan bagi menjaga keselamatan maklumat.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Menggunakan kemudahan *password screen saver* atau *log out* apabila meninggalkan komputer;<br>(b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan<br>(c) Memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat. | Pengguna |
| **Capaian/ Akses Pengguna** | **Tanggungjawab** |
| Capaian/ Akses Pengguna melibatkan aktiviti muat naik, muat turun dan penggunaan untuk tujuan yang dibenarkan. | Pengguna |

| | |
|---|---|
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Sebarang bahan yang dimuat turun daripada Internet hendaklah digunakan untuk tujuan yang dibenarkan; dan<br><br>(b) Pengguna adalah **DILARANG** melakukan aktiviti-aktiviti seperti berikut:<br><br>i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen serta sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian Internet; dan<br><br>ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah, jenayah atau pernyataan berbentuk hasutan tanpa kebenaran berbuat demikian. | |
| **Kawalan Capaian/ Akses Rangkaian**<br><br>**Objektif:** Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian. | |
| **Capaian/ Akses Rangkaian** | **Tanggungjawab** |
| Kawalan capaian perkhidmatan rangkaian adalah bagi menjamin keselamatan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Menempatkan atau memasang antara muka yang bersesuaian antara rangkaian MDM/ Jabatan/ Agensi di | Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT MDM/ Jabatan/ |

| | |
|---|---|
| bawah MDM, rangkaian agensi lain dan rangkaian awam;<br>(b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya;<br>(c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT;<br>(d) Mentadbir dan mengawal capaian Pengguna jarak jauh (remote user) dengan kebenaran bertulis;<br>(e) Mentadbir dan mengawal rangkaian yang dikongsi (shared networks), terutama sekali yang keluar daripada rangkaian MDM/ Jabatan/ Agensi di bawah MDM; dan<br>(f) Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan menempatkan atau memasang perkakasan ICT yang bersesuaian di rangkaian MDM/ Jabatan/ Agensi di bawah MDM. | Agensi di bawah MDM |
| **Capaian/ Akses Internet** | **Tanggungjawab** |
| Capaian internet bagi urusan rasmi membolehkan Pengguna berhubung dan mencapai maklumat dalam persekitaran yang selamat.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Pemantauan secara berterusan dilakukan bagi memastikan penggunaannya hanya untuk capaian yang dibenarkan sahaja;<br>(b) Penguatkuasaan *Content Filtering* hendaklah dilaksanakan bagi mengawal akses Internet mengikut fungsi kerja dan | ,<br>Pentadbir Rangkaian dan Komunikasi ICT MDM/ Jabatan/ Agensi di bawah MDM dan Pengguna |

| | |
|---|---|
| pemantauan tahap pematuhan;<br>(c) Pengawalan penggunaan *bandwidth* hendaklah dilaksanakan bagi penggunaan *bandwidth* yang maksimum dan lebih berkesan;<br>(d) Penggunaan Internet hanyalah untuk kegunaan rasmisahaja;<br>(e) Pengguna hanya dibenarkan memuat turun perisian yang sah dan berdaftar;<br>(f) Perolehan/ pembelian dan penggunaan *broadband* bergantung kepada justifikasi atau keperluan dan perlu mendapat kelulusan Pengurusan MDM/ Jabatan/ Agensi di bawah MDM; dan<br>(g) Penggunaan kemudahan internet peribadi di pejabat seperti modem, hotspot dan sebagainya untuk tujuan sambungan ke Internet adalah perlu mendapat kelulusan jika melibatkan sambungan ke rangkaian MDM/ Jabatan/ Agensi di bawah MDM. | |

**Kawalan Capaian/ Akses Sistem Pengoperasian**

**Objektif:** Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.

| Capaian/ Akses Sistem Pengoperasian | Tanggungjawab |
|---|---|
| Sistem Pengoperasian membolehkan Kawalan Capaian Sistem Pengoperasian bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian kepada sumber sistem komputer. | Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT |

| | |
|---|---|
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Mengawal capaian ke atas sistem pengoperasian menggunakan mekanisme log masuk yang terjamin;<br><br>(b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;<br><br>(c) Mengehadkan dan mengawal penggunaan perisian;<br><br>(d) Mengehadkan tempoh penggunaan dan/ atau sambungan ke sesebuah aplikasi berisiko tinggi;<br><br>(e) Mengesahkan Pengguna yang dibenarkan selaras dengan peraturan MDM/ Jabatan/ Agensi di bawah MDM; dan<br><br>(f) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian. | MDM/<br>Jabatan/<br>Agensi di bawah<br>MDM<br>dan<br>Pengguna |
| **Kawalan Capaian/ Akses Sistem Aplikasi dan Maklumat**<br><br>**Objektif:** Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat dalam sistem aplikasi. | |
| **Capaian/ Akses Sistem Aplikasi dan Maklumat** | **Tanggungjawab** |
| Capaian sistem aplikasi dan maklumat adalah terhad kepada Pengguna dan tujuan yang dibenarkan sahaja.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Penggunaan sistem aplikasi yang dibenarkan adalah mengikut ketetapan kawalan capaian, tahap capaian dan keselamatan yang telah ditentukan; | Pentadbir<br>Sistem ICT<br>MDM/<br>Jabatan/<br>Agensi di bawah<br>MDM<br>dan<br>Pengguna |

| | |
|---|---|
| (b) Memastikan jejak audit dan sistem log dilaksanakan bagi setiap aktiviti capaian sistem aplikasi dan maklumat;<br><br>(c) Mengehadkan capaian sistem aplikasi dan maklumat kepada tiga (3) kali percubaan. Sekiranya gagal, akaun pengguna akan disekat;<br><br>(d) Mengawal capaian ke atas sistem aplikasi dan maklumat menggunakan prosedur log masuk yang selamat, kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah;<br><br>(e) Capaian sistem aplikasi dan maklumat melalui capaian internet adalah dibenarkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja; dan<br><br>(f) Capaian kepada sistem aplikasi di MDM/ Jabatan/ Agensi di bawah MDM hendaklah mempunyai ciri-ciri keselamatan (contoh penggunaan *Secure Socket Layer* (SSL): https). | |
| **Peralatan Mudah Alih dan Kerja Jarak Jauh**<br><br>**Objektif:** Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh. | |
| **Kawalan Peralatan Mudah Alih** | **Tanggungjawab** |
| Peralatan mudah alih yang boleh mengumpul, merakam, menyiar dan menyampaikan maklumat dalam apa jua bentuk rekod elektronik perlu diberi kawalan perlindungan bagi memastikan keselamatan maklumat.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut: | Pegawai Aset MDM/ Jabatan/ Agensi di bawah MDM dan Pengguna |

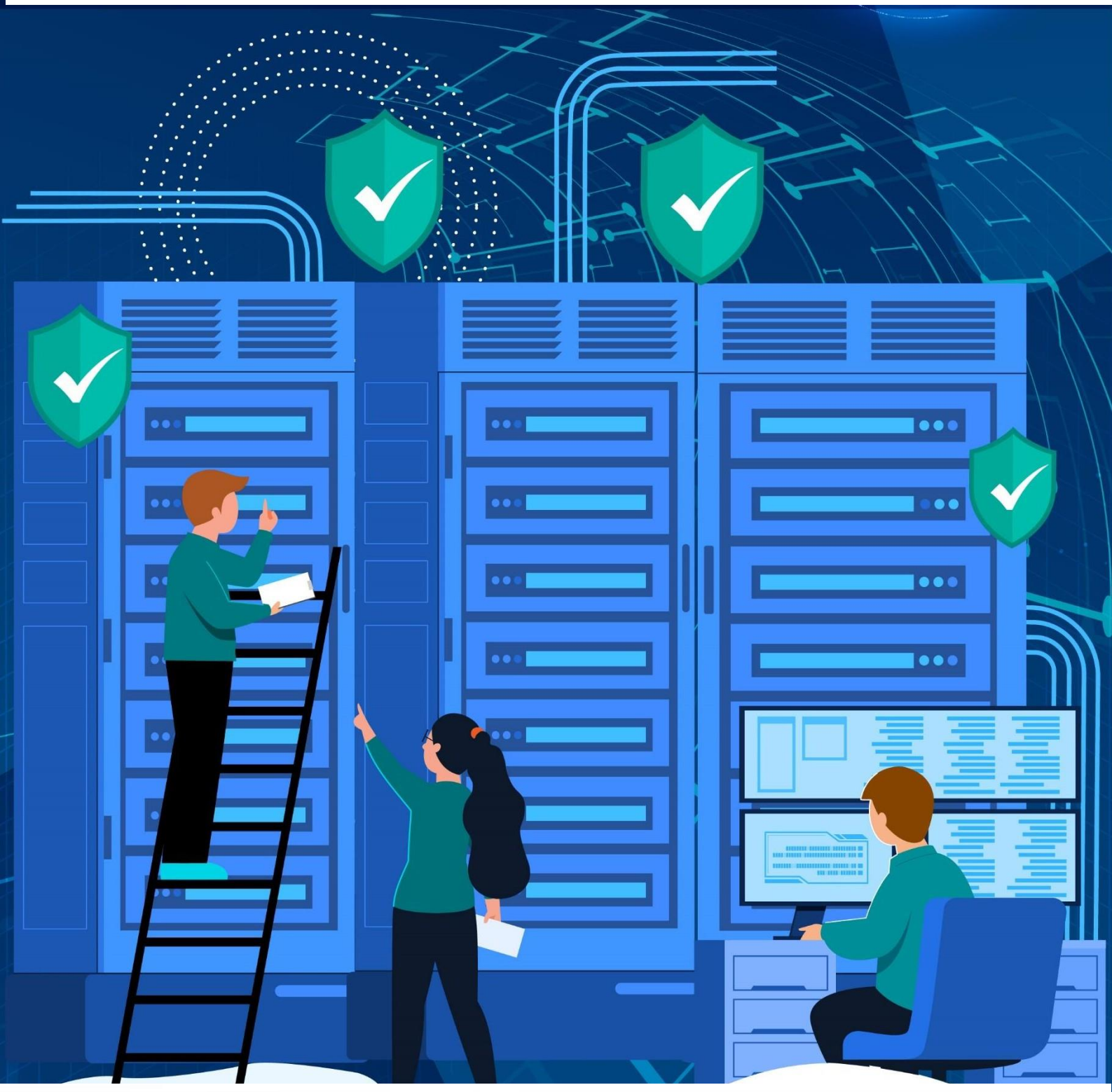
| | |
|---|---|
| (a) Semua Pengguna bertanggungjawab sepenuhnya terhadap pengurusan dan kawalan keselamatan setiap peralatan mudah alih yang dibekalkan;<br><br>(b) Rekod penggunaan peralatan mudah alih hendaklah diwujudkan, dikemaskini dan diperiksa;<br><br>(c) Memastikan peralatan mudah alih dihindari daripada sebarang ancaman, keselamatan maklumat seperti pendedahan, kecurian, pengubahsuaian dan pemalsuan;<br><br>(d) Peralatan mudah alih tidak disimpan di dalam kenderaan tanpa pengawasan, di tempat-tempat awam dan premis/ kawasan yang tidak selamat; dan<br><br>(e) Peralatan mudah alih yang didapati hilang hendaklah diuruskan berdasarkan kepada pekeliling semasa yang berkuatkuasa. | |
| **Kawalan Kemudahan Kerja Jarak Jauh** | **Tanggungjawab** |
| Kawalan Kemudahan Kerja Jarak Jauh adalah bagi memastikan tiada berlakunya kehilangan peralatan, pendedahan maklumat dan capaian tidak sah dan salah guna kemudahan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil untuk melindungi dari risiko penyalahgunaan peralatan mudah alih dan kemudahan komunikasi;<br><br>(b) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat; dan | Pengguna |

| | |
|---|---|
| (c) Untuk capaian dari luar rangkaian MDM/ Jabatan ke rangkaian dalaman mestilah menggunakan *Virtual Private Network* (VPN). | |
| ***Bring Your Own Device* (BYOD)**<br>**Objektif:** Memastikan keselamatan maklumat semasa menggunakan peralatan BYOD di MDM/ Jabatan/ Agensi di bawah MDM. | |
| **Keperluan dan Kawalan Penggunaan BYOD** | **Tanggungjawab** |
| Penggunaan BYOD yang disambungkan kepada rangkaian MDM/ Jabatan/ Agensi di bawah MDM sama ada menyimpan atau mengakses data rasmi Kerajaan adalah tertakluk kepada keperluan dan kawalan penggunaan BYOD.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Pengguna perlu mengetahui risiko dan kesan penggunaan BYOD terhadap keselamatan maklumat;<br>(b) Pengguna perlu mengetahui peraturan-peraturan yang telah ditetapkan apabila menggunakan BYOD;<br>(c) Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada penggunaan BYOD;<br>(d) Pendaftaran ke atas peralatan mudah alih;<br>(e) Keperluan ke atas perlindungan secara fizikal;<br>(f) Kawalan ke atas pemasangan perisian peralatan mudah alih;<br>(g) Kawalan ke atas versi dan *patches* perisian;<br>(h) Sekatan ke atas akses perkhidmatan maklumat secara | Pengguna |

| | |
|---|---|
| dalam talian;<br>(i) Kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptograf; dan<br>(j) Peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan. | |

# KESELAMATAN FIZIKAL DAN PERSEKITARAN

MAJLIS DAERAH MARANG



## KESELAMATAN FIZIKAL DAN PERSEKITARAN

| **Keselamatan Kawasan dan Persekitaran**<br><br>**Objektif:** Melindungi premis dan aset ICT daripada sebarang bentuk pencerobohan, kerosakan, ancaman, gangguan persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian, kecurian atau kemalangan serta akses yang tidak dibenarkan. | |
|---|---|
| **Kawalan Kawasan** | **Tanggungjawab** |
| Kawalan Kawasan bertujuan menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;<br><br>(b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan dan lain-lain) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;<br><br>(c) Melindungi kawasan terhad melalui kawalan-kawalan tertentu seperti memasang alat penggera, kamera litar tertutup atau EMS sekiranya berkaitan;<br><br>(d) Mengehadkan jalan keluar masuk;<br><br>(e) Mengadakan kaunter kawalan;<br><br>(f) Menyediakan ruang menunggu atau ruang kerja untuk Pihak Ketiga (jika perlu); | TM<br>MDM |

| | |
|---|---|
| (g) Mewujudkan perkhidmatan kawalan keselamatan;<br>(h) Melindungi kawasan terperingkat melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;<br>(i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam ruang dan bilik pejabat serta kemudahan yang disediakan;<br>(j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana;<br>(k) Menyediakan garis panduan untuk warga yang bekerja di dalam kawasan terperingkat; dan<br>(l) Memastikan kawasan-kawasan penghantaran dan pemunggahan serta tempat-tempat lain dikawal daripada pihak yang tidak diberi kebenaran memasukinya. | |
| **Kawalan Persekitaran** | **Tanggungjawab** |
| Kawalan persekitaran bertujuan menghindar kerosakan dan capaian terhadap peralatan ICT dan peralatan rangkaian bagi keselamatan maklumat agensi.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Memastikan susun atur semua aset ICT di Pusat Data adalah teratur dan kemas;<br>(b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan peralatan perlindungan keselamatan yang bersesuaian dan dibenarkan seperti alat pengesan kebakaran, alat pencegah | Jabatan/ dan Pengguna |

| | |
|---|---|
| kebakaran dan pintu kecemasan;<br>(c) Semua bahan mudah terbakar, cecair, bahan atau peralatan lain yang boleh merosakkan peralatan ICT hendaklah diletakkan di tempat yang bersesuaian dan berjauhan daripada aset ICT;<br>(d) Dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran aset ICT;<br>(e) Memastikan akses kepada saluran *riser* sentiasa dikunci;<br>(f) Memastikan peralatan rangkaian seperti *switch*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; dan<br>(g) Memastikan pegawai yang bertanggungjawab menyimpan semua kunci yang berkenaan dapat dihubungi apabila keadaan memerlukan berbuat demikian. | |
| **Kawalan Masuk Fizikal** | **Tanggungjawab** |
| Kawalan masuk fizikal bertujuan mengawal akses oleh pihak-pihak Pengguna, Pembekal dan Pihak Ketiga bagi keselamatan maklumat organisasi.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Pas keselamatan hendaklah dipakai sepanjang waktu bertugas;<br>(b) Semua pas keselamatan hendaklah diserahkan semula kepada MDM/ Jabatan/ Agensi di bawah MDM apabila Pengguna berhenti, bersara atau berpindah keluar;<br>(c) Pihak Ketiga hendaklah menyerahkan semula pas pelawat kepada MDM/ Jabatan/ Agensi di bawah MDM apabila | MDM,<br>PK<br>MDM/<br>Jabatan/<br>Agensi di bawah<br>MDM,<br>Pengguna,<br>Pembekal<br>dan<br>Pihak Ketiga |

| | |
|---|---|
| urusan selesai atau tamat kontrak;<br>(d) Pas pelawat hendaklah diambil di kaunter masuk. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan<br>(e) Kehilangan pas keselamatan/ pelawat mestilah dilaporkan dengan segera kepada KPK MDM/ Pegawai Keselamatan Jabatan/ Agensi di bawah MDM. | |
| **Kawasan Larangan** | **Tanggungjawab** |
| Kawasan Larangan dilaksanakan untuk melindungi aset ICT. Kawasan larangan ICT di MDM/ Jabatan/ Agensi di bawah MDM adalah Pusat Data/ Bilik Server/ Stor ICT.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja. Tanda kawasan larangan hendaklah dipamerkan;<br>(b) Buku log keluar/ masuk Pusat Data sentiasa dipantau dan diselenggara;<br>(c) Pihak Ketiga dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal;<br>(d) Pihak Ketiga hendaklah diiringi dan dipantau sepanjang masa oleh pegawai yang diberi kebenaran untuk mengakses Pusat Data sehingga tugas di kawasan berkenaan selesai. Pihak Ketiga juga perlu mematuhi semua peraturan Pusat Data yang ditetapkan; dan<br>(e) Peralatan rakaman/ penyimpanan seperti kamera, video, | TM<br>MDM<br>Jabatan<br>Agensi di bawah MDM,<br>Pembekal<br>dan<br>Pihak Ketiga |

| | |
|---|---|
| perakam suara dan storan mudah alih adalah tidak dibenarkan dibawa masuk ke dalam Pusat Data kecuali dengan kebenaran Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT. | |
| **Bekalan Kuasa** | **Tanggungjawab** |
| Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada aset ICT.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Semua peralatan ICT hendaklah dilindungi daripada kegagalan bekalan kuasa;<br>(b) Peralatan sokongan seperti *UPS* dan *Genset* boleh digunakan bagi perkhidmatan kritikal supaya mendapat bekalan kuasa berterusan; dan<br>(c) Semua peralatan sokongan bekalan kuasa hendaklah diperiksa, diuji dan diselenggara secara berjadual. | MDM/<br>Jabatan/<br>Agensi di bawah<br>MDM |
| **Kabel** | **Tanggungjawab** |
| Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat terdedah.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;<br>(b) Melindungi kabel daripada kerosakan yang disengajakan | TM<br>MDM |

| | |
|---|---|
| atau tidak disengajakan;<br>(c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan<br>(d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat. | |
| **Prosedur Kecemasan Bencana** | **Tanggungjawab** |
| Prosedur Kecemasan Bencana merupakan prosedur yang diwujudkan dan dipatuhi apabila berlaku insiden kecemasan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Memastikan setiap Pengguna memahami dan mematuhi **Prosedur Kecemasan Bencana**;<br>(b) Insiden kecemasan persekitaran mesti dilaporkan; dan<br>(c) Merancang dan menyertai latihan kecemasan bencana yang diadakan di MDM/ Jabatan/ Agensi di bawah MDM. | TM MDM/ Pengguna |
| **Keselamatan Peralatan**<br><br>**Objektif:** Melindungi peralatan ICT MDM/ Jabatan/ Agensi di bawah MDM daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut. | |
| **Peralatan ICT** | **Tanggungjawab** |
| Pengguna yang diberikan peralatan ICT hendaklah menjaga dan bertanggungjawab sepenuhnya ke atas peralatan ICT tersebut. | Pegawai Aset, Pentadbir |

| | |
|---|---|
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna.<br><br>(b) Melaporkan sebarang kerosakan peralatan ICT melalui saluran yang ditetapkan;<br><br>(c) Bertanggungjawab sepenuhnya ke atas peralatan ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran dan perubahan konfigurasi yang telah ditetapkan;<br><br>(d) Dilarang sama sekali menambah, mengganti atau mengeluarkan sebarang perkakasan ICT yang telah ditetapkan;<br><br>(e) Dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Peralatan ICT;<br><br>(f) Bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;<br><br>(g) Memastikan perisian antivirus yang dibekalkan di komputer peribadi/ komputer riba sentiasa aktif (active) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan. Pengguna dilarang untuk menyahpasang (uninstall) antivirus yang telah dipasang (installed);<br><br>(h) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;<br><br>(i) Semua peralatan sokongan ICT (aksesori) hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; | Peralatan ICT<br>MDM/<br>Jabatan/<br><br>dan<br><br>Pengguna |

| | |
|---|---|
| (j) Peralatan-peralatan kritikal perlu disokong oleh UPS;<br><br>(k) Semua peralatan ICT hendaklah disimpan atau diletakkandi tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan;<br><br>(l) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai;<br><br>(m) Peralatan ICT yang hendak dibawa keluar dari premis MDM/ Jabatan/ Agensi di bawah MDM hendaklah mematuhi peraturan yang telah ditetapkan;<br><br>(n) Peralatan ICT yang hilang hendaklah dilaporkan kepada PICT dan Pegawai Aset MDM/ Jabatan/ Agensi di bawah MDM dengan segera;<br><br>(o) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;<br><br>(p) Pengguna tidak dibenarkan mengalih kedudukan peralatan ICT dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset MDM/ Jabatan/ Agensi di bawah MDM. Perpindahan peralatan ICT hendaklah mematuhi peraturan yang telah ditetapkan;<br><br>(q) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;<br><br>(r) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;<br><br>(s) Bertanggungjawab terhadap peralatan ICT di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; | |

| | |
|---|---|
| (t) Memastikan semua peralatan ICT yang tidak digunakan dalam keadaan tutup (off) apabila meninggalkan pejabat;<br>(u) Memastikan plag dicabut daripada suis utama (main switch) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat; dan<br>(v) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada PICT. | |
| **Media Storan** | **Tanggungjawab** |
| Media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian mengikut kategori maklumat;<br>(b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja;<br>(c) Semua media storan perlu dikawal bagi mencegah daripada capaian yang tidak dibenarkan, kecurian dan kemusnahan;<br>(d) Langkah-langkah pencegahan hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat;<br>(e) Semua media storan yang mengandungi data kritikal hendaklah disimpan di tempat yang mempunyai ciri-ciri | TM<br>MDM /<br>dan Pengguna |

| | |
|---|---|
| keselamatan dengan mengikut prosedur yang telah ditetapkan;<br><br>(f) Mematuhi prosedur pengurusan media storan yang telah dikenal pasti termasuk akses, inventori, pergerakan, pelabelan serta *backup* dan *restore*;<br><br>(g) Perkakasan backup hendaklah diletakkan di tempat yang terkawal;<br><br>(h) Mengadakan salinan atau *backup* pada media storan kedua bagi tujuan keselamatan dan mengelakkan kehilangan data. Media storan kedua hendaklah disimpan di tempat yang selamat;<br><br>(i) Semua maklumat dalam media storan yang hendak dilupuskan mestilah dihapuskan terlebih dahulu. Proses pelupusan hendaklah dilakukan dengan teratur dan selamat mengikut prosedur pelupusan;<br><br>(j) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan<br><br>(k) Sebarang kehilangan media storan yang berlaku hendaklah dilaporkan mengikut peraturan semasa yang ditetapkan. | |
| **Media Sijil Digital** | **Tanggungjawab** |
| Sijil Digital terdapat dalam tiga (3) medium iaitu Token, *Roaming* dan *SoftCert.*<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media sijil digital daripada kecurian, kehilangan, | Pengguna |

| | |
|---|---|
| kerosakan, penyalahgunaan dan pengklonan;<br>(b) Token hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain;<br>(c) Perkongsian penggunaan token adalah tidak dibenarkan sama sekali;<br>(d) Media ini tidak boleh dipindah milik atau dipinjamkan; dan<br>(e) Sebarang kehilangan media sijil digital yang berlaku hendaklah dilaporkan mengikut peraturan semasa yang ditetapkan. | |
| **Media Perisian** | **Tanggungjawab** |
| Media perisian merupakan *disk*/ media yang digunakan apabila perisian diedarkan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan MDM/ Jabatan/ Agensi di bawah MDM; dan<br>(b) Lesen perisian (registration code, serials dan CD-keys) perlu disimpan berasingan daripada *CD-ROM*, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak. | MDM/<br>Jabatan<br>MDM<br>Pengguna |
| **Penyelenggaraan Peralatan ICT** | **Tanggungjawab** |
| Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. | Pentadbir<br>Peralatan ICT<br>MDM/ |

| | |
|---|---|
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Semua peralatan ICT yang diselenggara hendaklah mengikut spesifikasi yang telah ditetapkan;<br><br>(b) Memastikan peralatan ICT hanya boleh diselenggara oleh Pentadbir Peralatan ICT atau Pembekal atau Pihak Ketiga yang dibenarkan sahaja;<br><br>(c) Penyelenggaraan melibatkan perkakasan ICT dalamtempoh jaminan atau telah habis tempoh jaminan;<br><br>(d) Menyemak dan menguji semua peralatan ICT sebelum dan selepas proses penyelenggaraan; dan<br><br>(e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan. | Pengguna, Pembekal dan Pihak Ketiga |
| **Peralatan ICT Dibawa Keluar Dari Premis** | **Tanggungjawab** |
| Peralatan ICT yang dibawa keluar dari premis MDM/ Jabatan/ Agensi di bawah MDM adalah terdedah kepada pelbagai risiko.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Peralatan ICT termasuk perisian dan maklumat perlu dilindungi dan dikawal sepanjang masa;<br><br>(b) Penyimpanan atau penempatan peralatan ICT mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan<br><br>(c) Kehilangan peralatan ICT perlu dilaporkan mengikut prosedur pengurusan aset yang ditetapkan. | TM MDM ,Pengguna, Pembekal dan Pihak Ketiga |

| Pelupusan Peralatan ICT | Tanggungjawab |
|---|---|
| Pelupusan melibatkan peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki yang dibekalkan.<br><br>Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Peralatan ICT yang hendak dilupuskan perlulah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;<br><br>(b) Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT;<br><br>(c) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut prosedur pelupusan semasa yang berkuat kuasa; dan<br><br>(d) Pengguna adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:<br><br>i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan. Contoh: CPU, RAM, *hardisk, motherboard* dan sebagainya;<br>ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan; dan<br>iii. Memindah keluar dari lokasi mana-mana peralatan ICT yang | Pegawai Aset MDM/ Jabatan/ TM dan Pengguna |

| | |
|---|---|
| hendak dilupuskan. | |
| **Pindahan Peralatan ICT** | **Tanggungjawab** |
| Pindahan melibatkan semua peralatan ICT yang masih berkeadaan baik.<br><br>Peralatan ICT yang hendak dipindahkan mestilah mendapat kelulusan bertulis daripada Ketua Jabatan antara Bahagian/ Jabatan pemberi dan Bahagian/ Jabatan penerima.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Peralatan ICT yang hendak dipindahkan perlulah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;<br><br>(b) Pegawai Aset bertanggungjawab merekodkan butir-butir pindahan dan mengemas kini rekod pindahan peralatan ICT;<br><br>(c) Pindahan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut Tatacara Pengurusan Aset Alih Kerajaan yang sedang berkuatkuasa; dan<br><br>(d) Pengguna adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:<br><br>i. Menyimpan mana-mana peralatan ICT yang hendak dipindahkan. Contoh: CPU, RAM, hardisk,*motherboard* dan sebagainya;<br>ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan; dan<br>iii. Memindah keluar dari lokasi mana-mana peralatan ICT yang hendak dipindahkan. | Pegawai Aset MDM/ Jabatan/ dan Pengguna |

| Keselamatan Dokumen<br><br>**Objektif:** Melindungi maklumat MDM MDM/ Jabatan/ Agensi di bawah MDM daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian, pencerobohan, kemalangan atau kecurian. | |
|---|---|
| **Dokumen** | **Tanggungjawab** |
| Dokumen mengandungi Maklumat Rasmi atau Maklumat Terperingkat hedaklah didaftar, dikelas (dikelaskan sebagai Rahsia Besar, Rahsia, Sulit atau Terhad), dikelas semula dan dilupus dengan mematuhi peraturan yang sedang berkuat kuasa.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Setiap dokumen hendaklah difailkan dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;<br><br>(b) Pergerakan fail dan dokumen (termasuk pergerakan ke luar dari premis MDM/ Jabatan/ Agensi di bawah MDM) hendaklah dikawal dan direkodkan serta perlu mengikut prosedur keselamatan;<br><br>(c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan Kerajaan yang sedang berkuatkuasa;<br><br>(d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa; dan<br><br>(e) Penyimpanan maklumat rasmi di storan dalam talian diluar kawalan MDM/ Jabatan/ Agensi di bawah MDM adalah tidak dibenarkan. | Pengguna |

# KESELAMATAN OPERASI

MAJLIS DAERAH MARANG

## KESELAMATAN OPERASI

| | |
|---|---|
| **Pengurusan Prosedur Operasi**<br>**Objektif:** Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan. | |
| **Pengendalian Prosedur** | **Tanggungjawab** |
| Prosedur adalah dasar yang mengatur pengoperasian sistem maklumat.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumenkan, disimpan dan dikawal;<br><br>(b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan<br><br>(c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan. | TM<br>MDM |
| **Kawalan Perubahan** | **Tanggungjawab** |
| Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi. | Pemilik Sistem<br>TM<br>MDM |

| | |
|---|---|
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada Pemilik Sistem dan/ atauPICT dan/ atau Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT terlebih dahulu;<br><br>(b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana perkakasan ICT hendaklah dikendalikan oleh Pentadbir Peralatan ICT dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;<br><br>(c) Semua aktiviti pengubahsuaian aset ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan<br><br>(d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak. | |
| **Pengasingan Tugas dan Tanggungjawab** | **Tanggungjawab** |
| Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Skop tugas dan tanggungjawab termasuk mewujud, memadam, mengemas kini, mengubah dan mengesahkan perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan, akses atau pengubahsuaian yang tidak | TM<br>MDM |

| | |
|---|---|
| dibenarkan ke atas aset ICT daripada ralat, kebocoran maklumat terperingkat atau dimanipulasi;<br><br>(b) Aset ICT yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan daripada aset ICT yang digunakan sebagai persekitaran sebenar (production). Pengasingan juga merangkumi tindakan memisahkan antara kumpulan pembangun sistem dan pelaksana operasi; dan<br><br>(c) Pengasingan tugas bagi tugasan yang bersifat kritikal tidak boleh dilaksanakan oleh seorang individu sahaja atas kuasa tunggalnya dan hendaklah dikendalikan dalam tadbir urus yang bersesuaian. | Agensi di bawah MDM |
| **Pengurusan Penyampaian Perkhidmatan Pembekal dan Pihak Ketiga**<br><br>**Objektif:** Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat serta penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan Pembekal dan Pihak Ketiga. | |
| **Perkhidmatan Penyampaian ICT** | **Tanggungjawab** |
| Untuk mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal.<br><br>Perkara-perkara yang mesti dipatuhi adalah seperti berikut:<br><br>(a) Memastikan definisi perkhidmatan kawalan keselamatan, tahap penyampaian dan penyelenggaraan yang terkandung dalam perjanjian dipatuhi, dilaksanakan oleh Pembekal dan Pihak Ketiga; | TM<br>MDM |

| | |
|---|---|
| (b) Memantau perkhidmatan dan menyemak laporan serta rekod yang dikemukakan oleh Pembekal dan Pihak Ketiga;<br><br>(c) Mengurus sebarang perubahan terhadap pembekalan perkhidmatan dengan mengambil kira tahap kritikal perkhidmatan dan proses yang terlibat serta melaksanakan penilaian semula risiko keselamatan; dan<br><br>(d) Pelan kontigensi perlu disediakan bagi memastikan kesediaan kemudahan pemprosesan maklumat bagi perkhidmatan kritikal yang disediakan oleh Pembekal dan Pihak Ketiga. | Pembekal<br>dan<br>Pihak Ketiga |
| **Perancangan dan Penerimaan Sistem Aplikasi**<br><br>**Objektif:** Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem aplikasi. | |
| **080301 Perancangan Kapasiti** | **Tanggungjawab** |
| Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem aplikasi yang dikehendaki dicapai.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br><br>(a) Kapasiti sesuatu komponen atau sistem aplikasi hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan, kegunaan dan operasi sistem aplikasi pada masa akan datang; dan<br><br>(b) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti | Pemilik Sistem,<br>Pentadbir<br>Sistem ICT<br>MDM/<br>TM |

| | |
|---|---|
| gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang. | |
| **Penerimaan Sistem Aplikasi** | **Tanggungjawab** |
| Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br><br>(a) Semua sistem aplikasi baharu (termasuklah sistem aplikasi yang dikemas kini atau diubah suai) hendaklah memenuhi kriteria yang ditetapkan dan juga mengikut garis panduan yang sedang berkuatkuasa sebelum diterima atau dipersetujui; dan<br><br>(b) Sistem aplikasi baharu hendaklah menjalani proses imbasan keselamatan dan melaksanakan tindakan pengukuhan sebelum digunakan. | Pemilik Sistem, Jabatan/ MDM |

| **Perisian Berbahaya**<br><br>**Objektif:** Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *malware* dan sebagainya. | |
|---|---|
| **Perlindungan Dari Perisian Berbahaya** | **Tanggungjawab** |
| Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan *malware* hendaklah dilaksanakan dan digabungkan dengan kesedaran Pengguna terhadap serangan tersebut.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, IDS dan IPS serta memastikan prosedur penggunaan yang betul dan selamat diikuti;<br><br>(b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;<br><br>(c) Mengimbas peralatan ICT dengan antivirus sebelum digunakan;<br><br>(d) Mengemas kini antivirus dengan paten antivirus yang terkini;<br><br>(e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;<br><br>(f) Melaksanakan program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;<br><br>(g) Memasukkan klausa tanggungan di dalam kontrak pembekal | Pentadbir Sistem ICT, Jabatan/ MDM dan Pengguna |

| | |
|---|---|
| perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;<br><br>(h) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus; dan<br><br>(i) Penggunaan *MobileCode* hendaklah daripada sumber yang dipercayai dan daripada perisian yang telah mendapat jaminan kualiti sahaja. | |
| ***Housekeeping***<br><br>**Objektif:** Melindungi integriti maklumat agar boleh diakses pada bila-bila masa. | |
| ***Backup* dan *Restore*** | **Tanggungjawab** |
| Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di *off site.*<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Melaksanakan *backup* keselamatan ke atas semua perisian aplikasi dan sistem aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;<br><br>(b) Melaksanakan *backup* ke atas semua data dan maklumat mengikut keperluan. Kekerapan *backup* bergantung pada tahap kritikal maklumat dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi; | Pentadbir Sistem ICT Jabatan MDM |

| | |
|---|---|
| (c) *Backup* hendaklah dilakukan di dalam media yang bersesuaian;<br><br>(d) Menguji secara berkala prosedur dan media *backup* dan *restore* bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila perlu digunakan;<br><br>(e) Membangun dan melaksana pengurusan generasi backup berdasarkan pelan pengurusan risiko bagi setiap aset ICT;<br><br>(f) Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat; dan<br><br>(g) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan atau tahunan. | |
| **Pengurusan Rangkaian**<br><br>**Objektif:** Melindungi maklumat dalam rangkaian dan infrastruktur sokongan. | |
| **Kawalan Infrastruktur Rangkaian** | **Tanggungjawab** |
| Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi sistem dan aplikasi dalam rangkaian daripada ancaman.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;<br><br>(b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas daripada | TM<br>MDM |

| | |
|---|---|
| risiko seperti banjir, gegaran dan habuk;<br>(c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;<br>(d) Peralatan keselamatan seperti *firewall* hendaklah dipasang bagi memastikan hak capaian ke atas sistem aplikasi dapat dilaksanakan;<br>(e) Semua trafik keluar dan masuk hendaklah ditapis oleh peralatan keselamatan;<br>(f) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran;<br>(g) Memasang perisian IPS bagi mengesan sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam sistem aplikasi dan maklumat MDM/ Jabatan/ Agensi di bawah MDM; dan<br>(h) Sebarang penyambungan rangkaian yang bukan di bawah kawalan MDM/ Jabatan/ Agensi di bawah MDM adalah tidak dibenarkan. | |
| **Pengurusan Media**<br>**Objektif:** Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan. | |
| **Pengurusan Media Boleh Alih** | **Tanggungjawab** |
| Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh MDM/ Jabatan/ Agensi di bawah MDM. . | Pentadbir |

| | |
|---|---|
| Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;<br><br>(b) Mengehadkan dan menentukan capaian media kepada Pengguna yang dibenarkan sahaja;<br><br>(c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;<br><br>(d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan;<br><br>(e) Menyimpan semua media di tempat yang selamat;<br><br>(f) Media yang mengandungi maklumat terperingkat hendaklah dilupuskan mengikut prosedur yang telah ditetapkan; dan<br><br>(g) Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Pentadbir Peralatan ICT terlebih dahulu. | Peralatan ICT<br>MDM/<br>Jabatan/ dan<br>Pengguna |
| **Pemindahan Media Fizikal** | **Tanggungjawab** |
| Senarai syarikat kourier/ pemindah yang diluluskan perlu diselenggara dan prosedur pengenalan syarikat kourier/ pemindah perlu diwujudkan. Log identiti bagi maklumat, masa pemindahan dan resit perlu diselenggara yang merupakan sebahagian dari prosedur tersebut.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Pelupusan media fizikal perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh | Pegawai Aset<br>dan<br>Pentadbir<br>Peralatan ICT |

| | |
|---|---|
| Kerajaan; dan<br><br>(b) Media fizikal yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa. | |
| **Keselamatan Sistem Dokumentasi** | **Tanggungjawab** |
| Sistem dokumentasi adalah merupakan komponen komunikasi, kawalan dan pemantauan dalam fasa pengurusan projek seperti pembangunan sistem, pengoperasian sistem dan penyelenggaraan sistem.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;<br><br>(b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan<br><br>(c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada. | Pentadbir Sistem ICT Jabatan/ MDM |

| Keselamatan Pengkomputeran Awan | |
|---|---|
| **Objektif:** Mengawal data dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang oleh penyedia perkhidmatan. Perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. | |
| **Pengurusan Pengkomputeran Awan** | **Tanggungjawab** |
| Pengurusan pengkomputeran awan merupakan proses pemantauan dan memastikan keberkesanan dalam penggunaan pengkomputeran awam secara *public*, *private* atau *hybrid*.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Memastikan penyedia perkhidmatan memenuhi keselamatan siber, kerahsiaan dan kebolehpercayaan;<br><br>(b) Menyediakan perjanjian perkhidmatan di antara MDM/ Jabatan/ Agensi di bawah MDM dengan penyedia perkhidmatan;<br><br>(c) Memastikan SLA dilaksanakan (jika berkaitan); dan<br><br>(d) Memastikan tiada kebocoran dan penyalahgunaan data. | TM<br>MDM |

| Perkhidmatan E-Dagang (Electronic Commerce Services)<br><br>**Objektif:** Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang. | |
|---|---|
| **E-Dagang** | **Tanggungjawab** |
| Proses menjalankan urusan perniagaan (membeli atau menjual barangan atau perkhidmatan) melalui rangkaian komputer atau internet.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan;<br><br>(b) Maklumat yang terlibat dalam transaksi dalam talian (on-line) sama ada menggunakan *private cloud*, *public cloud* atau *hybrid cloud* perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan;<br><br>(c) Maklumat yang melibatkan transaksi dalam talian perlu dilindungi bagi mengelakkan transmisi yang tidak lengkap, mis-routing, pendedahan, pertindihan dan perubahan yang tidak dibenarkan; dan<br><br>(d) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan. | Pentadbir Sistem dan Pengguna |

| | |
|---|---|
| **Pemantauan**<br><br>**Objektif:** Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan. | |
| **081001 Pengauditan dan Forensik ICT** | **Tanggungjawab** |
| Pengauditan dan forensik ICT merupakan proses mengenalpasti bahan bukti fizikal dengan menggunakan teknologi dan sains forensik.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Memastikan jadual pelaksanaan disediakan;<br>(b) Memastikan laporan dapatan dilaksanakan;<br>(c) Memastikan tindakan pembetulan dilaksanakan; dan<br>(d) Memastikan kemudahan penyimpanan log dan maklumat log dilindungi daripada pengubahan tidak sah dan capaian tanpa izin. | MDM<br>TM |
| **Jejak Audit** | **Tanggungjawab** |
| Jejak audit sistem ICT adalah merupakan bukti yang didokumenkan dan adalah merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Memastikan maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; | TM<br>MDM/<br>Jabatan/ |

| | |
|---|---|
| (b) Jejak audit ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap akses yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan;<br><br>(c) Jejak audit hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling semasa yang berkuatkuasa; dan<br><br>(d) Jejak audit hendaklah dikawal bagi mengekalkan integriti data. Analisis ke atas jejak audit hendaklah dilakukan bagi mengesan:<br><br>i. Kegagalan capaian;<br>ii. Penggunaan yang tidak normal, contoh: akses terhadap sistem di luar waktu kebiasaan, kekerapan akses dan tempoh penggunaan yang berlainan dari kebiasaan;<br>iii. Capaian ke atas rekod-rekod terhad; dan<br>iv. Transaksi yang mencurigakan. | Agensi di bawah MDM |
| **Sistem Log dan Pemantauan** | **Tanggungjawab** |
| Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem komputer ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem.<br><br>Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti• aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan.<br><br>Log hendaklah disimpan dan direkodkan selaras dengan arahan/ pekeliling terkini yang dikeluarkan oleh Kerajaan. Log | Pentadbir Sistem ICT MDM/ Jabatan MDM |

| | |
|---|---|
| hendaklah dikawal bagi mengekalkan integriti data. Jenis fail log bagi *server* dan aplikasi yang perlu diaktifkan adalah seperti yang berikut:<br><br>i. Fail log sistem pengoperasian;<br><br>ii. Fail log servis (contoh: web, e-mel);<br><br>iii. Fail log aplikasi (audit trail); dan<br><br>iv. Fail log rangkaian (contoh: *switch*, *firewall,* IPS).<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;<br><br>(b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera;<br><br>(c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, aktiviti ini hendaklah dilaporkan kepada ICTSO dan PICT;<br><br>(d) Pemantauan berterusan boleh dibuat secara automatik dengan menggunakan perisian tertentu sebagai contoh pengimbas virus, algoritma *check sum, password cracker*, semakan integriti, pengesanan penceroboh dan analisis pemantauan prestasi sistem komputer; dan<br><br>(e) Teknologi yang digunakan untuk pemantauan berterusan boleh ditempatkan secara berpusat bagi menjalankan analisis terhadap log yang dikumpulkan dari pelbagai sistem. | |

| Penyeragaman Jam (Clock Synchronization) | Tanggungjawab |
|---|---|
| Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal.<br><br>Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MDM atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh *National Metrology Institute of Malaysia* (NMIM). | MDM/ Jabatan/ |
| **Media Sosial**<br><br>**Objektif:** Memastikan keselamatan dan kawalan penyebaran maklumat melalui media sosial. | |
| **Keselamatan Media Sosial** | **Tanggungjawab** |
| Keselamatan media sosial merupakan proses menyingkirkan ancaman keselamatan melalui pemantauan keselamatan siber.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Tidak menjejaskan kepentingan perkhidmatan awam dan kedaulatan negara;<br><br>(b) Tidak melibatkan penyebaran maklumat dan dokumen terperingkat;<br><br>(c) Tidak memaparkan kenyataan yang boleh menjejaskan imej Kerajaan;<br><br>(d) Tidak menyentuh isu sensitif seperti agama, politik dan perkauman; | Pentadbir Media Sosial MDM/ Jabatan/ dan Pengguna |

| | |
|---|---|
| (e) Tidak memaparkan kenyataan yang berunsur fitnah atau hasutan;<br>(f) Tidak menyebarkan berita yang tidak sahih;<br>(g) Tidak melibatkan diri dengan aktiviti yang boleh menjurus kepada *CyberStalking* atau *CyberHarassment*;<br>(h) Tidak menggunakan media sosial untuk tujuan peribadi semasa waktu pejabat sama ada menerusi peralatan komputer/ peranti mudah alih yang dibekalkan oleh Kerajaan;<br>(i) Mematuhi dasar dan peraturan semasa berkaitan media sosial yang sedang berkuatkuasa; dan<br>(j) Memastikan keselamatan media sosial dengan melaporkan masalah yang berlaku seperti spam dan pencerobohan kepada penyedia perkhidmatan media sosial. | |
| **Data Terbuka**<br>**Objektif:** Data Terbuka bertujuan meningkatkan kualiti dan ketelusan penyampaian perkhidmatan kerajaan menerusi perkongsian data yang tepat, cepat dan relevan selaras dengan inisiatif kerajaan. | |
| **Pengurusan Data Terbuka** | **Tanggungjawab** |
| Pengurusan data terbuka MDM/ Jabatan/ Agensi di bawahMDM perlulah berasaskan tadbir urus dan aktiviti semasa yang berkuatkuasa.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Pewujudan struktur tadbir urus untuk melaksanakan tugas dan aktiviti berkaitan data terbuka yang merangkumi Jawatankuasa Penyelarasan Data Terbuka dan Pasukan | Analitis Data Raya MDM<br>dan<br>Pasukan Kerja Data Terbuka |

| | |
|---|---|
| Kerja Data Terbuka;<br>(b) Membangunkan dan melaksanakan **Pelan Pelaksanaan Data Terbuka MDM**; dan<br>(c) Melaksanakan pemantauan secara berkala berkaitan pelaksanaan data terbuka MDM/ Jabatan/ Agensi di bawah MDM. | MDM/ Jabatan/ Agensi di bawah MDM |
| **Data Raya**<br>**Objektif:** Memanfaatkan penggunaan data dan pembuatan keputusan dalam penyampaian perkhidmatan berasaskan analisis data raya bagi meningkatkan hasil dan mengurangkan kos kerajaan. | |
| **Pengurusan Data Raya** | **Tanggungjawab** |
| Pengurusan data raya MDM perlulah berasaskan tadbir urus serta arahan semasa yang sedang berkuatkuasa.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Mewujudkan struktur tadbir urus untuk melaksanakan tugas dan aktiviti berkaitan data raya MDM;<br>(b) Membangunkan dan melaksanakan Pelan Pelaksanaan Projek (mengikut keperluan projek sedia ada atau baharu); dan<br>(c) Melaksanakan pemantauan secara berkala berkaitan dengan pelaksanaan data raya MDM. | Jawatankuasa Penyelarasan Data Terbuka, PMO<br>Analitis Data Raya MDM<br>dan<br>Pasukan Kerja Data Terbuka MDM/ Jabatan/ Agensi di bawah MDM |

# KESELAMATAN KOMUNIKASI

MAJLIS DAERAH MARANG

## BIDANG 09: KESELAMATAN KOMUNIKASI

| **Pengurusan Keselamatan Rangkaian**<br>**Objektif:** Memastikan maklumat dan kemudahan dalam rangkaian dilindungi. | |
|---|---|
| **Kawalan Rangkaian** | **Tanggungjawab** |
| Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman bagi MDM/ Jabatan/ Agensi di bawah MDM.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan;<br><br>(b) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir, gegaran dan habuk;<br><br>(c) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja;<br><br>(d) Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;<br><br>(e) *Firewall* hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT;<br><br>(f) Semua trafik keluar dan masuk rangkaian hendaklah melalui *firewall* di bawah kawalan MAMPU;<br><br>(g) Semua trafik keluar dan masuk rangkaian di Pusat Data dan pejabat-pejabat cawangan hendaklah melalui *firewall* di bawah kawalan Pentadbir Pusat Data, Rangkaian dan | Pentadbir Sistem ICT MDM/ Jabatan/ Agensi di bawah MDM |

| | |
|---|---|
| Komunikasi ICT;<br><br>(h) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer Pengguna;<br><br>(i) Digalakkan memasang perisian bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat seperti berikut:<br><br>i. IPS;<br>ii. *Web Content Filtering*; dan<br>iii. IDS.<br><br>(j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT adalah tidak dibenarkan;<br><br>(k) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di MDM sahaja dan penggunaan rangkaian luar adalah dengan kelulusan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT;<br><br>(l) Kemudahan bagi *wireless* LAN hendaklah dipantau dan dikawal penggunaannya;<br><br>(m) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan;<br><br>(n) Menempatkan atau memasang antara muka (interface) yang bersesuaian di antara rangkaian MDM/ Jabatan/ Agensi di bawah MDM, rangkaian agensi lain dan rangkaian awam;<br><br>(o) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; | |

| | |
|---|---|
| (p) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian yang dibenarkan sahaja;<br><br>(q) Mengawal capaian fizikal dan logikal ke atas kemudahan *port* diagnostik dan konfigurasi jarak jauh;<br><br>(r) Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan MDM/ Jabatan/ Agensi di bawah MDM; dan<br><br>(s) Mewujud dan melaksana kawalan pengalihan laluan (routing control) bagi memastikan pematuhan terhadap kawalan capaian MDM/ Jabatan/ Agensi di bawah MDM. | |
| **Keselamatan Perkhidmatan Rangkaian** | **Tanggungjawab** |
| Pengurusan bagi semua perkhidmatan rangkaian (inhouse atau outsource) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti. Mekanisme keselamatan dan tahap perkhidmatan hendaklah dimasukkan di dalam perjanjian perkhidmatan rangkaian.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Komponen keselamatan rangkaian merangkumi perkakasan, perisian dan perkhidmatan perkomputeran awan digunakan bagi memastikan rangkaian selamat dari ancaman, serangan siber, cubaan pengodaman dan kecuaian Pengguna;<br><br>*(b)* Sistem Keselamatan Rangkaian menggunakan kombinasi pelbagai komponen keselamatan rangkaian bagi membentuk sistem pertahanan berlapis/ *a layered defense* | ,Pentadbir Sistem ICT MDM/ Jabatan/ Agensi di bawah MDM, Pembekal dan Pihak Ketiga |

| | |
|---|---|
| *system*; dan<br><br>(c) Setiap lapisan sistem pertahanan membekal keupayaan pemantauan, pengenalan dan pemulihan bagi memastikan rangkaian selamat. | |
| **Pengasingan Dalam Rangkaian** | **Tanggungjawab** |
| Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian MDM/ Jabatan/ Agensi di bawah MDM.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Mengenal pasti fungsi dan tanggungjawab pengguna;<br><br>(b) Mengkonfigurasi hak capaian pengguna mengikut segmen rangkaian berdasarkan keperluan;<br><br>(c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;<br><br>(d) Mengemaskinikan hak capaian pengguna dari semasa ke semasa mengikut keperluan; dan<br><br>(e) Operasi rangkaian hendaklah diasingkan untuk meminimumkan risiko capaian dan pengubahsuaian yang tidak dibenarkan. | Pentadbir Sistem ICT MDM/ Jabatan/ Agensi di bawah MDM |

| Pemindahan/ Pertukaran Data dan Maklumat<br>**Objektif:** Memastikan keselamatan perpindahan/ pertukaran data, maklumat dan perisian antara MDM/ Jabatan dan pihak luar terjamin. | |
|---|---|
| **Polisi dan Prosedur Pemindahan/ Pertukaran Data dan Maklumat** | **Tanggungjawab** |
| MDM/ Jabatan/ Agensi Di bawah MDM perlu mengambil kira keselamatan maklumat apabila berlaku pemindahan data dan maklumat organisasi antara MDM/ Jabatan/ Agensi di bawah MDM dengan pihak luar.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Mewujudkan polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi;<br><br>(b) Menyediakan perjanjian atau kebenaran bertulis untuk pertukaran maklumat dan perisian di antara MDM/ Jabatan dengan pihak agensi luar;<br><br>(c) Melindungi media yang mengandungi maklumat daripada capaian yang tidak dibenarkan, didedahkan, disalah guna atau dirosakkan semasa pemindahan keluar dari MDM/ Jabatan; dan<br><br>(d) Memastikan maklumat yang terdapat dalam mel elektronik hendaklah dilindungi sebaik-baiknya. | Pentadbir Sistem ICT, MDM/ Jabatan/ dan Pengguna |

| Perjanjian Mengenai Pemindahan/ Pertukaran Data dan Maklumat | Tanggungjawab |
|---|---|
| MDM/ Jabatan/ Agensi di bawah MDM perlu mengambilkira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan/ pertukaran data dan maklumat organisasi antara MDM/ Jabatan/ Agensi Di bawah MDM dengan pihak luar.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Mengawal penghantaran dan penerimaan maklumat;<br>(b) Memastikan prosedur keupayaan mengesan dan tanpa sangkalan semasa pemindahan/ pertukaran data dan maklumat;<br>(c) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan/ pertukaran data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan<br>(d) Mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data. | Pemilik Sistem<br>MDM<br>TM |
| **Pesanan Elektronik** | **Tanggungjawab** |
| Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa yang sedang berkuatkuasa.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Penggunaan pesanan elektronik disediakan untuk | Pengguna |

| | |
|---|---|
| memudahkan komunikasi antara Pengguna, Pembekal dan Pihak Ketiga hanya untuk kegunaan bisnes dengan sekatan-sekatan tertentu;<br>(b) Penghantaran e-mel dan kepilan tidak berkaitan tugas rasmi harian adalah dilarang;<br>(c) Mesej yang dihantar hendaklah ringkas dan ditujukan kepada yang berkenaan sahaja;<br>(d) Mesej yang dihantar tidak menggunakan akaun orang lain melainkan dengan arahan yang telah ditetapkan; dan<br>(e) Pengguna dilarang mengulang hantar/ *forward* maklumat terhad tanpa kebenaran penghantar/ pemunya maklumat. | |
| **Pengurusan E-mel** | **Tanggungjawab** |
| E-mel merupakan surat, pesanan atau mesej dalam bentuk fail komputer yang dikirim dan diterima melalui sistem rangkaian komputer.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Menggunakan akaun e-mel yang diperuntukkan oleh MDM/ Jabatan sahaja sebagai e-mel rasmi;<br>(b) Memastikan pengemaskinian peti e-mel (mailbox) dilaksanakan supaya kapasiti e-mel tidak melebihi kuota yang telah ditetapkan;<br>(c) Menggunakan akaun e-mel rasmi untuk tujuan tugas rasmi sahaja;<br>(d) Mengambil tindakan dan memberi maklum balas segera terhadap e-mel; dan | Pengguna |

| | |
|---|---|
| (e) Memastikan e-mel rasmi yang dihantar atau diterima disimpan mengikut prosedur pengurusan sistem fail elektronik yang telah ditetapkan. | |
| **Pengurusan Komunikasi Bersepadu (UC)** | **Tanggungjawab** |
| Perkhidmatan komunikasi dan kolaborasi bersepadu yang diuruskan secara berpusat. Perkhidmatan ini menggabungkan saluran-saluran komunikasi e-mel, persidangan video dan audio, *instant messaging* serta Sistem Pengurusan Identiti.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Memastikan setiap komunikasi yang dibuat untuk tujuan rasmi sahaja;<br>(b) Melindungi maklumat rahsia rasmi dan maklumat rasmi Kerajaan;<br>(c) Memastikan maklumat yang dihantar mengikut etika keselamatan yang ditetapkan; dan<br>(d) Akaun yang diperuntukkan oleh MDM/ Jabatan/ Agensi di bawah MDM sahaja yang boleh digunakan. | Pengguna |
| **Perjanjian Kerahsiaan atau Ketakdedahan** | **Tanggungjawab** |
| Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan MDM/ Jabatan/ Agensi di bawah MDM dan hendaklah disemak dan didokumentasikan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Setiap orang yang terlibat dengan Maklumat Rahsia | Pentadbir Sistem ICT MDM/ Jabatan/ Agensi di bawah |

| | |
|---|---|
| Rasmi, hendaklah menandatangani perjanjian ketakdedahan seperti Arahan Keselamatan Kerajaan yang sedang berkuatkuasa. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan; dan<br>(b) Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka. | MDM, Pembekal dan Pengguna |

# PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN SIBER

BIDANG 12

PENGURUSAN PENGENDALIAN
INSIDEN KESELAMATAN SIBER

MAJLIS DAERAH MARANG

## PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN SIBER

| **Mekanisme Pelaporan Insiden Keselamatan Siber**<br>**Objektif:** Memastikan insiden keselamatan siber dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan siber. | |
|---|---|
| **Mekanisme Pelaporan Insiden** | **Tanggungjawab** |
| Insiden keselamatan siber hendaklah dilaporkan kepada ICTSO dan CERT MDM dengan kadar segera.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Melaporkan insiden keselamatan siber apabila:<br>i. Maklumat disyaki/ didapati hilang atau terdedah kepada pihak-pihak yang tidak diberi kuasa;<br>ii. Sistem komputer disyaki atau digunakan tanpa kebenaran;<br>iii. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan;<br>iv. Berlaku kejadian yang luar biasa kepada sistem komputer seperti kehilangan fail, sistem komputer kerap kali gagal dan komunikasi tersalah hantar; dan<br>v. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden keselamatan maklumat yang tidak dijangka.<br><br>Ringkasan bagi semua proses kerja yang terlibat dalam Pelaporan Insiden Keselamatan Siber di MDM seperti **LAMPIRAN 3.** | Pemilik Sistem, Pentadbir Sistem ICT Jabatan/ MDM dan Pengguna |

| **Pengurusan Maklumat Insiden Keselamatan Siber**<br>**Objektif:** Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan siber. | |
|---|---|
| **Prosedur Pengurusan Insiden Keselamatan Siber** | **Tanggungjawab** |
| Sebarang insiden keselamatan siber hendaklah dikawal dengan menggunakan **Prosedur Pengurusan Insiden Keselamatan Siber** yang telah ditetapkan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti;<br>(b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;<br>(c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan (sekiranya perlu); dan<br>(d) Melapor kepada NACSA apabila berlaku sebarang insiden keselamatan siber (sekiranya perlu). | CERT<br>MDM |