DASAR KESELAMATAN ICT

MAJLIS BANDARAYA KUANTAN

مجليس بانداراي كوانتن
MAJLIS BANDARAYA
KUANTAN
CITY COUNCIL

KANDUNGAN

1. PENGENALAN

Majlis Bandaraya Kuantan merupakan nadi pertumbuhan di Pantai Timur. Seiring dengan pembangunan dan pertumbuhan ini peranan MBK untuk mempermudahkan dan mempercepatkan proses pembangunan ini akan terlaksana melalui penggunaan ICT. Serentak dengan itu, Dasar ICT ini akan menjadi panduan bagi membantu dan membimbing para pegawai dan kakitangan yang bertanggungjawab untuk melaksanakan tugas serta program yang melibatkan ICT.

Selaras dengan peranan tersebut MBK telah melaksanakan projek pengkomputerannya bagi memastikan penyediaan perkhidmatan kepada pelanggan dapat dilakukan dengan pantas dan berkesan. Berdasarkan kepentingan di atas, pengurusan MBK telah mengeluarkan dokumen ini bagi memastikan objektif pengkomputeran ini tercapai. Dokumen ini mengandungi beberapa pernyataan dasar mengikut aspek-aspek penting dalam melindungi aset ICT di MBK. Ia menerangkan peraturan yang perlu dipatuhi oleh mereka yang mencapai teknologi maklumat dan data di MBK.

Tujuan utama dokumen ini ialah untuk memaklumkan kepada personel MBK tentang tanggungjawab dan peranan dalam melindungi aset-aset ICT.

2. PERNYATAAN DASAR, OBJEKTIF, SKOP DAN PRINSIP KESELAMATAN ICT

2.1 Pernyataan Dasar Keselamatan ICT

Dasar Keselamatan ICT MBK adalah untuk melindungi aset ICT dengan meminimumkan kesan insiden keselamatan. Ini adalah bertujuan untuk menjamin kesinambungan urusan dengan menekankan aspek kepenggunaan aset ICT serta prosedur keselamatan yang perlu diikuti seperti yang telah ditetapkan.

2.2 Objektif

Dasar Keselamatan ICT dibentuk bertujuan untuk :-

i. Menjamin semua aset ICT (termasuk maklumat elektronik dan bukan elektronik, perisian, data, rangkaian data dan peralatan) dan pengguna, peraturan, tanggungjawab serta kemudahan ICT yang terdapat di MBK adalah dilindungi sepenuhnya daripada kemusnahan, kehilangan, disalahgunakan atau penyelewengan.

ii. Membantu membimbing para pegawai dan kakitangan MBK menggunakan kaedah yang sistematik dan seragam dalam melaksanakan tugas-tugas dan tanggungjawab yang melibatkan ICT.

iii. Memastikan segala perkhidmatan akan berjalan dengan lancar dan berterusan.

iv. Melindungi kepentingan mereka yang bergantung pada teknologi maklumat, daripada kesan kegagalan ICT dari segi kerahsiaan, integriti, kebolehsediaan dan ‘tidak boleh disangkal’.

v. Mencegah salahguna dan kecurian aset ICT Jabatan.

2.3 Skop

Dasar ini merangkumi peralatan ICT serta semua bentuk maklumat elektronik yang bertujuan untuk menjamin kerahsiaan dan integriti maklumat tersebut serta kesahihan pengguna dan ketersediaan kepada semua pengguna yang dibenarkan.

Dasar ini adalah terpakai oleh semua pengguna di MBK termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, muat turun, muat naik, menyedia, berkongsi, menyimpan dan menggunakan aset ICT MBK

2.4 Prinsip-prinsip

MBK menerimapakai prinsip keselamatan ICT yang berikut :

a) Capaian Atas Dasar Perlu Mengetahui

Capaian terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna capaian hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk capaian

adalah berdasarkan kategori maklumat sepertimana yang dinyatakan di dalam dokumen “Arahan Keselamatan”

b) Hak Capaian Minimum

Hak capaian kepada pengguna hanya diberi pada tahap aset 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.

c) Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT MBK.

d) Pengasingan

Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

e) Pengauditan

Tujuan aktiviti ini ialah untuk mengenal pasti insiden keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, router, firewall dan rangkaian hendaklah menyelenggarakan jejak-jejak audit.

f) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui Backup dan peraturan pemulihan atau suatu Pelan Pemulihan Bencana dan Pelan Kesinambungan Perkhidmatan.

g) Pematuhan

Tujuan utama ialah untuk menghindar, mengesan, melengah dan bertindakbalas terhadap sebarang perlanggaran Dasar Keselamatan ICT MBK.

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 mekanisma keselamatan, dapat menjamin keselamatan yang maksimum.

3. PENGURUSAN KESELAMATAN ICT

3.1 Organisasi/Struktur Keselamatan ICT

Penglibatan pengurusan atasan adalah penting dalam merancang, menentu hala tuju, memantau keberkesanan dan membudayakan program keselamatan ICT.

Pelaksanaan dasar ini akan dijalankan oleh Datuk Bandar MBK dengan dibantu oleh Jawatankuasa Pemandu yang diketuai oleh Setiausaha Majlis (CIO) dan dianggotai oleh Pegawai Keselamatan ICT (ICTSO) serta wakil-wakil Jabatan.

3.2 Pengurusan Risiko

MBK melalui ICTSO akan melaksanakan penilaian risiko dari semasa ke semasa ke atas aset ICT jabatan bertujuan untuk memastikan ancaman, kelemahan dan risiko di MBK berada di tahap yang paling minimum.

3.3 Pengurusan Maklumat Sensitif

Pengurusan maklumat sensitif di MBK hendaklah mematuhi peraturan-peraturan yang telah ditetapkan di dalam Arahan Keselamatan. Maklumat sensitif yang dikirim secara elektronik hendaklah menggunakan sistem penyulitan yang diluluskan.

3.4 Pengurusan Virus

Memasang antivirus, mengemas kini versi antivirus dan melaksanakan aktiviti imbasan virus ke atas aset ICT yang berkaitan secara berterusan.

3.5 Pengurusan Kata Laluan

Pengurusan, pemilihan dan penggunaan kata laluan perlu mengikut panduan yang ditetapkan oleh MyMIS atau lain-lain amalan terbaik. Kata laluan hendaklah dilindungi dan tidak boleh dikongsi. Pengguna hendaklah mengubah katalaluan bagi setiap 6 bulan untuk mengelak katalaluan ini dikesan dan digunakan untuk menceroboh.

3.6 Pengurusan Capaian Internet

Penggunaan internet hendaklah dipantau secara berterusan supaya bahan atau laman web yang sesuai sahaja diakses. Dasar ini juga meliputi aktiviti muat turun (download), penggunaan internet untuk tugas rasmi dan menapis laman web yang tidak sesuai.

3.7 Pengurusan Mel Elektronik (E-mel)

Penggunaan e-mel hendaklah dipantau secara berterusan bagi memenuhi keperluan etika penggunaan, langkah-langkah perlindungan dan penguatkuasaan yang ditetapkan oleh BTM, agar penggunaan e-mel dapat dikawal dan tahap keselamatan sistem komunikasi dokumen rasmi kerajaan terjamin.

3.8 Keselamatan Perkakasan dan Perisian

Melindungi semua perkakasan dan perisian dari sebarang ancaman,kelemahan dan risiko. BTM perlu memantau penggunaannya bagi mengelakkan penyalahgunaan. BTM perlu memastikan bahawa perisian yang digunakan adalah tulen dan berlesen.

3.9 Keselamatan Komunikasi

Penghantaran dan penerimaan maklumat mestilah selamat dan terjamin dari segi integriti, kerahsiaan dan kesahihannya. ICTSO perlu mengawal sebarang aktiviti komunikasi.

3.10 Keselamatan Fizikal

Premis ICT perlu dilindungi dari sebarang bentuk ancaman seperti pencerobohan, kebakaran dan bencana alam. Sebarang pengubahsuaian terhadap premis aset ICT perlu dirujuk kepada ICTSO untuk kelulusan.

3.11 Keselamatan Dokumen dan Media

Semua dokumen dan media hendaklah diberi perlindungan keselamatan yang secukupnya. Dokumen dan media mesti diklasifikasikan mengikut keperluan, kepentingan dan tahap keselamatan. Sistem pengurusan dokumen dan media perlu diwujudkan bagi menerima, memproses, menyimpan, menghantar dan melupus.

3.12 Keselamatan Kad Pintar dan Kad Kedatangan

Setiap personel atau pengguna yang menggunakan kad pintar untuk menjalankan urusan perkhidmatan hendaklah memastikan keselamatan kad pintar dengan mengambil langkah-langkah perlindungan yang telah ditetapkan oleh Majlis. Majlis perlu mengawalselia dan memantau secara berterusan penggunaan kad pintar di MBK.

3.13 Keselamatan Pangkalan Data

Pangkalan data perlu dilindungi daripada capaian tanpa kebenaran dan semua bentuk kemusnahan. Semua capaian ke pangkalan data perlu mendapat kebenaran dari ICTSO.

3.14 Pelan Kesinambungan Perkhidmatan

Perkhidmatan perlu diteruskan walaupun berlaku sebarang bentuk kegagalan sistem dan kemusnahan. Oleh itu, MBK perlu mewujudkan pelan kesinambungan perkhidmatan dan diuji secara berkala.

3.15 Pengurusan Telekomunikasi

Pengguna yang ingin membuat capaian kepada aset ICT secara telekomunikasi perlu mendapat kelulusan dari ICTSO. Perkara utama yang perlu dipastikan ialah persekitaran talian pengguna adalah selamat daripada sebarang ancaman, kelemahan dan risiko.

3.16 Pengurusan Outsourcing

Projek ICT boleh diuruskan oleh pihak ketiga sekiranya diperlukan dan telah mendapat kelulusan. Pihak ketiga termasuk juruperunding dan pembekal terikat dengan perjanjian untuk memastikan integriti dan kerahsiaan maklumat. Kebocoran maklumat rahsia rasmi boleh dikenakan tindakan di bawah Akta Rahsia Rasmi 1972.

3.17 Kesedaran Keselamatan ICT

Semua personel dan pengguna hendaklah dididik menerima dan melaksanakan peraturan keselamatan ICT sebagai sebahagian dari kewajipan dalam perkhidmatan. Program kesedaran keselamatan ICT hendaklah diwujud dan dilaksanakan di MBK.

3.18 Pelaporan Insiden Keselamatan ICT

Sebarang insiden keselamatan mestilah dilaporkan kepada GCERT MAMPU. Prosedur operasi standard perlu disediakan oleh MBK dan diletakkan di bawah tanggungjawab CIO dan ICTSO. Tindakan selanjutnya akan diputuskan oleh Pengarah Jabatan.

3.19 Pengendalian Perubahan

a) Penyerahan Tugas dan Tanggungjawab

Penyerahan tugas dan tanggungjawab hendaklah dilaksanakan secara rasmi apabila berlaku perubahan personel berkaitan dengan ICT.

b) Perubahan Konfigurasi Sistem ICT

Sebarang bentuk perubahan konfigurasi sistem yang melibatkan aset ICT Jabatan mestilah direkod dan dikemaskinikan.

4. PERUNDANGAN

4.1 Penguatkuasaan

Semua pengguna dikehendaki memahami dan mematuhi semua peraturan-peraturan yang terkandung dalam Dasar Keselamatan ICT MBK.

4.2 Pelanggaran Dasar Keselamatan ICT

Pelanggaran Dasar Keselamatan ICT akan dirujuk dan dilapor kepada ICTSO. Perkara ini boleh dirujuk kepada Lembaga Tatatertib dan sekiranya melibatkan unsur jenayah dilapor kepada pihak berkuasa.

5. PENYELENGGARAAN DOKUMEN

5.1 Pengendalian Perubahan Dokumen

Dasar keselamatan ICT tertakluk kepada perubahan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur perundangan dan kepentingan sosial. Dasar ini hendaklah dibaca bersama dengan dokumen-dokumen yang berkaitan dengan standard, garis panduan dan langkah keselamatan ICT Kerajaan yang akan dikeluarkan dari semasa ke semasa.

5.2 Pemberitahuan Perubahan

Sebarang perubahan terhadap dasar keselamatan ICT hendaklah dimaklumkan kepada semua personel dan pengguna.

5.3 Cadangan Pindaan

Sebarang cadangan pindaan berkaitan dengan dasar ini hendaklah dikemukakan kepada ICTSO.

Nama : Puan Nurul Ashikin binti Ahmad Khairudin
Pegawai Keselamatan ICT (ICTSO)

Alamat : Majlis Bandaraya Kuantan
Kompleks Bandaraya Kuantan
Jalan Tanah Putih
25100 Kuantan
Pahang Darul makmur
Telefon : 09 – 5121555
Emel : sheekin@mbk.gov.my

5.4 Penyemakan Semula

Dasar Keselamatan ICT tertakluk kepada semakan dan pindaan. Penyemakan semula hendaklah dilaksanakan oleh ICTSO dari semasa ke semasa selaras dengan perubahan dasar Kerajaan, teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial.

Disediakan Oleh:

Bahagian Teknologi Maklumat

Majlis Bandaraya Kuantan

2022

LAMPIRAN 1

Carta Organisasi Struktur Keselamatan ICT MBK