GARIS PANDUAN KESELAMATAN DOKUMEN ELEKTRONIK DAN PENGURUSAN MEDIA

PERBADANAN MEMAJUKAN IKTISAD NEGERI TERENGGANU

1 JUN 2023

1.0 PENGENALAN

Peningkatan penggunaan ICT dalam tugasan harian terutama yang melibatkan penggunaan Internet dan e-mel telah mendedahkan maklumat penting kepada pihak luar. Perkembangan ICT dan peningkatan penyebaran virus, program jahat (*malicious code*), aktiviti kecurian identiti (*phishing*), pengodam (*hacking*), *spamming* dan sebagainya sewajarnya menyedarkan para pengguna agar lebih bertanggungjawab dalam menggunakan kemudahan ICT.

Untuk memastikan maklumat-maklumat penting bebas daripada sebarang ancaman, semua pengguna adalah disarankan untuk mematuhi Garis Panduan Keselamatan Dokumen Elektronik dan Pengurusan Media yang telah ditetapkan. Dokumen ini adalah untuk menjamin dan meningkatkan tahap keselamatan maklumat yang dicapai, dihantar, diterima atau dirujuk agar tidak dimanipulasi.

Dokumen Elektronik meliputi e-mel dan semua data serta maklumat yang disimpan di media storan merangkumi disket, *Compact Disk* (CD), USB *drive* (*thumb drive / flash drive*) *hard disk* dan lain-lain media yang boleh menyimpan dokumen elektronik.

2.0 OBJEKTIF

Tujuan utama Garis Panduan Keselamatan Dokumen Elektronik dan Pengurusan Media ini diwujudkan adalah sebagai panduan untuk pengguna demi menjamin kesinambungan urusan kerajaan dan menghindari kesan daripada insiden keselamatan. Dalam era ICT masa kini keselamatan dokumen dan maklumat menjadi perkara utama untuk diberi perhatian bagi mengelakkan daripada disalahgunakan oleh pihak yang tidak bertanggungjawab. Dokumen atau maklumat amat berharga kerana kebanyakan informasi tersebut boleh menjadi sensitif dan dikategorikan sebagai Maklumat Terperingkat.

Penyalahgunaan aset ICT oleh pihak yang tidak bertanggungjawab bukan sahaja memberi ruang kepada kebocoran maklumat malah menjejaskan maruah organisasi dan negara. Justeru, garis panduan ini diwujudkan supaya menjadi panduan kepada para pengguna ICT agar kesahihan, keutuhan, dan kebolehsediaan maklumat yang berterusan sentiasa terjamin.

3.0 KESELAMATAN ICT

Garis Panduan Keselamatan Dokumen Elektronik dan Pengurusan Media ini bertujuan untuk menjamin dan meningkatkan tahap keselamatan maklumat yang dicapai, dihantar, diterima ataupun dirujuk tidak dimanipulasi.

Garis panduan ini juga diharapkan dapat menjamin keselamatan dokuman atau maklumat organisasi dalam aspek-aspek seperti berikut:

a) Kerahsiaan (*Confidentiality*)

Sumber maklumat elektronik tidak boleh didedahkan sewenang-wenangnya atau dibiarkan dicapai tanpa kebenaran pihak berkuasa.

b) Integriti (*Integrity*)

Data dan maklumat hendaklah tepat, lengkap dikemaskini dan tidak berlaku sebarang manipulasi. Sebarang perubahan terhadap data dan maklumat hanya boleh dilakukan oleh pegawai yang telah diberikan kuasa untuk mengubah data/maklumat yang berkenaan dan mengikut prosedur yang dibenarkan.

c) Kesahihan (*Validity*)

Punca data dan maklumat hendaklah dari punca yang sah dan tanpa keraguan.

d) Tidak Boleh Disangkal (*Authenticity*)

Data atau maklumat hendaklah dijamin ketepatan, kesahihannya dan tidak boleh disangkal.

e) Kebolehsediaan (Availability)

Data dan maklumat hendaklah sentiasa boleh dicapai pada bila-bila masa oleh para pengguna yang sah.

4.0 KESELAMATAN DOKUMEN ELEKTRONIK

Perlindungan dokumen eletronik yang berterusan memerlukan kaedah penyelenggaraan, pengendalian dan penyimpanan dokumen elektronik aktif dan tidak aktif yang cekap dan berkesan.

4.1 TATACARA PENGURUSAN DOKUMEN ELEKTRONIK

Memelihara keselamatan dokumen rasmi kerajaan amat penting bagi semua dokumen. Sifat dokumen eletronik yang boleh dimanipulasikan bermakna bahawa dalam ketiadaan langkah keselamatan yang sesuai, amat mudah bagi mengubah atau menghapuskannya. Sebuhungan dengan ini, semua pengguna dikehendaki mengambil langkah-langkah berikut:

i. Dokumen rasmi yang dikategorikan sebagai terperingkat/penting **PERLU** dilindungi sekurang-kurangnya dengan katalaluan.

ii. Hanya pegawai yang dibenarkan sahaja boleh mengakses komputer/notebook/sistem aplikasi/ dokumen elektronik dan media storan yang mengandungi dokumen terperingkat.

iii. Memastikan fail aplikasi ditutup dan *log off* komputer/notebook sekiranya perlu meninggalkan stesen kerja.

iv. Memastikan komputer/notebook dilindungi dengan katalaluan mestilah minima 8 aksara gabungan teks, nombor dan aksara khas.

v. Penghantaran dokumen terperingkat melalui rangkaian perlulah menggunakan transaksi yang dienkrip.

vi. Menyimpan dokumen terperingkat ke storan Internet awam (*cloud*) contohnya seperti *OneDrive*, *DropBox*, *Google Drive* dan sebagainya adalah dilarang sama sekali.

vii. Dokumen terperingkat yang dihantar melalui e-mel perlu dienkrip terlebih dahulu sebelum dihantar dan pastikan penerima mengesahkan penerimaan e-mel yang dihantar. Penghantaran dokumen terperingkat melalui e-mel ke alamat selain daripada domain '@pmint.gov.my' perlu dilindungi oleh katalaluan yang diberikan secara berasingan kepada penerima.

viii. Pengguna dilarang daripada menggunakan e-mel persendirian untuk menghantar sebarang e-mel untuk tujuan urusan rasmi.

ix. E-mel yang mengandungi dokumen terperingkat tidak boleh dipanjangkan kepada penerima lain selain penerima yang berhak sahaja.

x. E-mel yang mengandungi dokumen terperingkat yang hendak dimusnahkan perlu dihapuskan secara kekal daripada folder *Trash* dengan melaksanakan '*Empty Trash*'.

xi. Memastikan dokumen-dokumen terperingkat dihapuskan sekiranya komputer/notebook terlibat dengan penggantian sebelum menyerahkannya kepada pihak ketiga.

5.0 KESELAMATAN MEDIA STORAN

Media storan seperti disket, *Compact Disk* (CD), USB *drive* (*thumb drive/flash drive*), *hard disk* dan lain-lain digunakan untuk menyimpan dokumen rasmi serta sebarang fail elektronik. Risiko dokumen rasmi yang disimpan dalam media storan adalah tinggi untuk terdedah kepada pihak-pihak yang tidak berkenaan.

5.1 TATACARA PENGURUSAN MEDIA STORAN

Untuk menjamin keselamatan media storan, anggota hendaklah mengikuti langkah - langkah berikut:

i. Media storan yang dibekalkan oleh Jabatan adalah untuk tujuan rasmi sahaja.

ii. Setiap media storan mudah alih perlu dilabelkan.

iii. Media storan yang mengandungi maklumat terperingkat mestilah diasing, disimpan dan diuruskan dengan selamat serta dilabelkan mengikut pengelasannya.

iv. Pegawai adalah **DILARANG** memberi atau meminjamkan media storan yang mengandungi maklumat rasmi kepada orang lain untuk mengelak daripada berlakunya kebocoran rahsia.

v. Penggunaan media storan peribadi untuk tujuan penyimpanan Salinan (*backup*) dokumen rasmi kerajaan adalah **DILARANG**.

vi. Media storan yang rosak atau tidak boleh digunakan lagi, perlulah dipadamkan semua data didalamnya menggunakan kaedah yang sesuai sebelum dilupuskan.

vii. Media storan yang memerlukan penyelenggaraan / penggantian oleh pihak ketiga perlu diformat terlebih dahulu atau lain-lain kaedah yang sesuai mengikut situasi untuk memastikan semua dokumen rasmi dalam media storan tersebut tidak terdedah kepada mana-mana pihak.

viii. Elakan media storan daripada terdedah kepada debu atau habuk, sinaran matahari, suhu panas, elektrostatik dan magnet serta disimpan di tempat yang selamat. ini dapat mengelakkan maklumat atau data menjadi rosak (*corrupted*) atau tidak boleh dibaca.

ix. *External hardisk / pen drive* mestilah dikeluarkan daripada sistem dengan cara yang betul. Pengguna **DILARANG** mengeluarkan secara terus darpada port USB.

x. Sekiranya media storan yang digunakan telah mencapai jangka hayat maksimum penggunaannya, kandungan fail atau maklumat di dalamnya perlu dipindahkan ke media storan baharu.

xi. Semua media storan luar hendaklah diimbas dengan perisian anti-virus dan anti-malware dari semasa ke semasa untuk mengelak penyebaran virus, cecacing atau program hasad ditanam ke dalam sistem rangkaian.

xii. Pegawai dikehendaki memulangkan semula media storan mudah alih milik kerajaan kepada pihak pentadbiran sekiranya bertukar atau meninggalkan perkhidmatan.

6.0 KEHILANGAN MEDIA STORAN DAN PELANGGARAN GARIS PANDUAN

Kehilangan media storan yang dibekalkan oleh Jabatan merupakan insiden keselamatan dan perlu dilaporkan kepada ICTSO Jabatan. Laporan taksiran analisis risiko perlu disediakan oleh Jabatan berkaitan mengikut arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa.

Jika media storan tersebut terbukti hilang, data / maklumat di dalam media storan tersebut bocor atau dimanipulasi atau disalah guna, Ketua Jabatan hendaklah menimbang sama ada tindakan tatatertib di bawah Peraturan-peraturan Pegawai Awam (Kelakuan dan Tatatertib) yang sedang berkuatkuasa atau penyiasatan di bawah akta-akta yang berkaitan periu diambil. Laporan polis kepada balai polis yang terdekat hendaklah dibuat sekiranya difikirkan sesuatu kesalahan jenayah telah berlaku.

7.0 PENUTUP

Secara ringkasnya, keselamatan dokumen elektronik dan media storan perlu dilaksanakan secara menyeluruh dan memerlukan kerjasama semua pihak. Aspek keselamatan merupakan tanggungjawab bersama dan tidak hanya dikhususkan kepada satu pihak sahaja. Melalui garis panduan ini diharapkan semua maklumat penting sentiasa berada dalam keadaan boleh dipercayai dan boleh dicapai pada bila- bila masa tanpa sebarang keraguan.