GARIS PANDUAN KESELAMATAN DOKUMEN ELEKTRONIK DAN MEDIA STORAN

PEJABAT SETIAUSAHA KERAJAAN NEGERI PULAU PINANG

GARIS PANDUAN KESELAMATAN DOKUMEN ELEKTRONIK DAN MEDIA STORAN

1.	**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 Media Storan yang telah ditetapkan. Garis Panduan Keselamatan Dokumen Elektronik dan Media Storan ini adalah untuk menjamin dan meningkatkan tahap keselamatan maklumat yang dicapai, dihantar, diterima atau dirujuk tidak dimanipulasi. Dokumen Elektronik meliputi e-mel dan semua data serta maklumat yang disimpan di media storan. Media Storan merangkumi disket, *Compact Disk* (CD), *USB drive (thumb drive/flash drive)*, *hard disk* dan lain-lain media yang boleh menyimpan dokumen elektronik.	Keperluan dan kepentingan garis panduan Definasi dokumen elektronik dan media storan
2.	**OBJEKTIF** Tujuan utama Garis Panduan Keselamatan Dokumen Elektronik dan Media Storan ini adalah sebagai panduan kepada para pengguna peralatan ICT dalam pentadbiran Negeri Pulau Pinang 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 mengelak daripada disalahgunakan oleh pihak yang tidak bertanggungjawab. Dokumen atau maklumat amat berharga kerana kebanyakan informasi tersebut boleh menjadi sensitif atau 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 itu, garis panduan ini diwujudkan supaya menjadi panduan kepada para pengguna ICT agar kesahihan, keutuhan dan kebolehsediaan maklumat yang berterusan sentiasa terjamin.	Tujuan garis panduan Kesan penyalahgunaan aset ICT

3.	**KESELAMATAN ICT** Garis panduan ini digubal bagi menjamin keselamatan 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.	Kerahsiaan Integriti Kesahihan Tidak boleh disangkal Kebolehsediaan
4.	**KESELAMATAN DOKUMEN ELEKTRONIK** Perlindungan dokumen elektronik 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 merupakan tanggungjawab yang amat penting kepada semua pengguna peralatan ICT. Sifat dokumen elektronik yang boleh dimanipulasikan bermakna bahawa dalam ketiadaan langkah keselamatan yang sesuai, amat mudah bagi mengubah atau menghapuskannya. Sehubungan dengan ini, semua pengguna peralatan ICT dikehendaki mengambil langkah-langkah berikut; **a. Dokumen** i. Dokumen rasmi yang dikategorikan sebagai terperingkat/penting **PERLU** dilindungi sekurang-kurangnya dengan katalaluan.	Keperluan memelihara keselamatan dokumen Kata laluan pada dokumen

	ii. Memastikan fail aplikasi ditutup dan *logoff* PC/*notebook* sekiranya perlu meninggalkan stesen kerja.	*Clear desk, clear screen*
	iii. Penghantaran dokumen terperingkat melalui rangkaian perlulah menggunakan transaksi yang dienkrip.	Penghantaran dokumen terperingkat melalui rangkaian
	iv. Menyimpan atau menghantar dokumen terperingkat ke storan Internet awam (cloud) contohnya seperti di *OneDrive, Dropbox, Google Drive* dan sebagainya adalah dilarang sama sekali.	Larangan menyimpan dokumen terperingkat di storan *Cloud*
	v. Memastikan dokumen-dokumen rasmi dihapuskan sekiranya PC/notebook terlibat dengan penggantian sebelum menyerahkannya kepada pihak ketiga.	Penghapusan dokumen pada PC/notebook yang perlu diganti
	b. Aset ICT	
	i. Hanya pegawai yang dibenarkan sahaja boleh mengakses PC/notebook/sistem aplikasi/ dokumen elektronik dan media storan yang mengandungi dokumen rasmi.	Kebenaran akses
	ii. Memastikan PC/notebook dilindungi dengan katalaluan minima lapan (8) aksara gabungan teks, nombor dan aksara khas.	Kata laluan pada PC/notebook
	c. e-Mel Rasmi	
	i. Dokumen rasmi yang dihantar melalui e-mel perlu dienkrip terlebih dahulu dan pastikan penerima mengesahkan penerimaan e-mel yang dihantar. Penghantaran dokumen rasmi melalui e-mel ke alamat selain daripada domain '@penang.gov.my' perlu sekurang-kurangnya dilindungi oleh kata laluan yang dikongsi secara berasingan dengan penerima.	Penghantaran dokumen terperingkat melalui e-mel
	ii. Pengguna dilarang daripada menggunakan akaun e-mel persendirian untuk menghantar sebarang e-mel untuk tujuan urusan rasmi.	Larangan penggunaan akaun e-mel peribadi
	iii. e-Mel yang mengandungi dokumen rasmi yang diterima tidak boleh dipanjangkan kepada pihak lain.	Larangan panjangkan e-mel terperingkat
	iv. e-Mel yang mengandungi dokumen rasmi yang ingin dimusnahkan perlu dihapuskan secara kekal daripada folder 'Trash' dengan melaksanakan 'Empty Trash'.	Penghapusan e-mel secara kekal
5.	**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.	Risiko mengunakan media storan
5.1	TATACARA PENGURUSAN MEDIA STORAN	
	Untuk menjamin keselamatan media storan, anggota hendaklah mengikuti langkah-langkah berikut:	Tatacara pengurusan media storan