SETIAUSAHA KERAJAAN NEGERI PULAU PINANG
Pejabat Setiausaha Kerajaan Negeri,
Paras 25, KOMTAR,
10503 Pulau Pinang

Telefon : 04-261 5613
Faxs : 04-261 8618
Laman Web : www.penang.gov.my

RUJ. KAMI:PSUKPP.BTMK.600-1/
5/3(18)

TARIKH : 3 J'awwal 1440
9 Januari 2019

Ketua-Ketua Jabatan Negeri
PULAU PINANG

Ketua-Ketua Badan Berkanun Negeri
PULAU PINANG

Ketua-Ketua Pengurusan Pihak Berkuasa Tempatan
PULAU PINANG

YB. Dato'/YBhg. Dato'/Tuan/Puan,

GARIS PANDUAN KESELAMATAN DOKUMEN ELEKTRONIK DAN MEDIA STORAN

Dengan hormatnya saya merujuk perkara di atas.

2. Penggunaan ICT dalam melaksanakan tugasan harian kini menjadi keperluan utama di semua jabatan atau agensi kerajaan. Ini menyebabkan seluruh anggota pentadbiran Kerajaan Negeri Pulau Pinang terdedah kepada risiko keselamatan ICT sekiranya dokumen elektronik dan media storan masing-masing tidak diuruskan dengan baik.

3. Garis Panduan Keselamatan Dokumen Elektronik dan Media Storan Kerajaan Negeri Pulau Pinang Versi 1.0 yang dikeluarkan pada 20 Ogos 2013 telah disemak semula dengan kerjasama Pejabat Ketua Keselamatan Kerajaan Negeri Pulau Pinang, Arkib Negeri Pulau Pinang dan ahli *Computer Eemergency Response* Team (CERT) Negeri Pulau Pinang.

4. Mesyuarat Jawatankuasa Pemandu Electronic Good Governance (JKP eGG) Bil. 4/2018 pada 21 November 2018 pada dasarnya telah

bersetuju dengan Garis Panduan Keselamatan Dokumen Elektronik dan Media Storan Kerajaan Negeri Pulau Pinang versi 1.1 yang telah dibentangkan.

5. Pemakaian garis panduan ini mula berkuatkuasa daripada tarikh surat ini dikeluarkan.

6. Sehubungan itu, kerjasama seluruh anggota pentadbiran Kerajaan Negeri Pulau Pinang adalah diharapkan untuk memantapkan amalan keselamatan terhadap semua dokumen elektronik dan media storan selaras dengan garis panduan ini.

Sekian, terima kasih.

"CEKAP, AKAUNTABILITI DAN TELUS"
"BERKHIDMAT UNTUK NEGARA"

Saya yang menjalankan amanah,

[DATO' SERI FARIZAN BIN DARUS]

s.k:

YAB Ketua Menteri,
Pulau Pinang.

e.d:

Timbalan Setiausaha Kerajaan Negeri (Pengurusan)
Timbalan Setiausaha Kerajaan Negeri (Pembangunan)
Semua Ketua Bahagian/Unit PSUKPP

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

	a. Tatacara umum	
	i. Media storan yang dibekalkan oleh jabatan adalah untuk menyimpan dokumen rasmi jabatan sahaja.	Tujuan media storan dibekalkan
	ii. Setiap media storan mudah alih perlu dilabelkan.	Label pada media storan
	iii. Media storan yang mengandungi dokumen rasmi perlu diasing, disimpan dan diuruskan dengan selamat serta dilabelkan mengikut pengelasannya. Jabatan perlu mewujudkan prosedur kawalan penggunaan yang bersesuaian.	Penyimpanan media storan yang mengandungi dokumen rasmi
	iv. Semua data di dalam media storan milik jabatan yang ingin dilupuskan perlu dipadam dengan sempurna menggunakan kaedah yang sesuai sebelum proses pelupusan dilaksanakan.	Pengendalian media storan jabatan yang perlu dilupuskan
	v. Media storan yang memerlukan penyelenggaraan / penggantian oleh pihak ketiga perlu diformat terlebih dahulu atau melaksanakan lain-lain kaedah yang sesuai mengikut situasi untuk memastikan semua dokumen rasmi dalam media storan tersebut tidak terdedah kepada mana-mana pihak.	Pengendalian media storan yang perlu diselenggara/ diganti
	vi. Elakkan 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 yang disimpan menjadi rosak (*corrupted*) atau tidak boleh dibaca.	Penjagaan fizikal media storan
	vii. *External hardisk / pen drive* perlu dikeluarkan daripada sistem dengan cara yang betul. Pengguna dilarang mengeluarkan secara terus daripada port USB.	Kaedah selamat untuk keluarkan media storan daripada PC/notebook
	viii. Sekiranya media storan yang digunakan telah mencapai jangka hayat maksimum penggunaannya, kandungan fail di dalamnya perlu dipindahkan ke media storan baharu.	Pengendalian media storan yang mencapai jangka hayat maksimum
	ix. 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.	Penjagaan media storan daripada serangan virus dan malware
	b. Tanggung jawab pegawai	
	i. Pegawai **DILARANG** memberi atau meminjamkan media storan yang mengandungi maklumat rasmi kepada orang lain untuk mengelak daripada berlakunya kebocoran maklumat.	Larangan memberi atau meminjamkan media storan kepada pihak lain
	ii. Pegawai **DILARANG** membawa keluar media storan yang mengandungi maklumat rasmi daripada premis kerajaan melainkan peraturan-peraturan berikut dipatuhi;	Pengecualian larangan bawa keluar media storan
	a. Mendapat kebenaran bertulis daripada Ketua Jabatan;	Tatacara membawa keluar media storan yang mengandungi dokumen rasmi
	b. Semua maklumat rasmi perlu melalui proses penyulitan; dan	
	c. Media storan tersebut hendaklah disimpan mengikut tatacara penyimpanan maklumat rasmi.	
	iii. Penggunaan media storan peribadi untuk tujuan penyimpanan salinan *(backup)* dokumen rasmi jabatan adalah **DILARANG**.	Larangan penggunaan media storan peribadi

	iv. Pegawai dikehendaki memulangkan semula media storan mudah alih milik kerajaan kepada pihak pentadbiran jabatan masing-masing sekiranya bertukar atau meninggalkan perkhidmatan.	Pengendalian media storan pegawai bertukar atau tamat perkhidmatan
6.	**KEHILANGAN MEDIA STORAN DAN PELANGGARAN GARIS PANDUAN** Kehilangan media storan yang dibekalkan oleh Kerajaan 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 berkuat kuasa atau penyiasatan di bawah akta-akta yang berkaitan perlu diambil. Laporan polis kepada balai polis yang terdekat hendaklah dibuat sekiranya difikirkan sesuatu kesalahan jenayah telah berlaku.	Tindakan sekirannya berlaku kehilangan media storan jabatan Tindakan Ketua Jabatan
7.	**KHIDMAT NASIHAT** Sebarang pertanyaan berkaitan garis panduan ini, sila hubungi: **Maklumat Perhubungan** Pentadbir Keselamatan dan Rangkaian — No Tel: 04-650 5630; Emel : pnet@penang.gov.my	Maklumat perhubungan
8.	**PENUTUP** Secara ringkasnya, keselamatan dokumen elektronik & media storan perlu dilaksanakan secara menyeluruh dan memerlukan kerjasama semua pihak. Aspek keselamatan merupakan tanggung jawab 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.	