BAHAGIAN AUDIT DALAM
JABATAN PERDANA MENTERI

SELF ASSESSMENT KEMUDAHAN ICT

TEMPOH PENILAIAN: 1 JULAI 2020 HINGGA 30 JUN 2021

Pejabat Yang Dinilai	:	Bahagian Teknologi Maklumat Jabatan .....
Perkara Yang Diaudit	:	Kawalan Kemudahan ICT
Objektif Audit	:	Untuk memastikan kawalan kemudahan ICT di senggara dengan baik dan sistematik.

Perkara yang dinilai dalam tempoh yang dinyatakan mengenai kawalan kemudahan ICT yang memerlukan makluman/ulasan/tindakan.

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
1.	Perisian komputer	Memastikan perisian yang diperoleh oleh Jabatan / Bahagian telah diterima dan digunakan selaras dengan pekeliling. Peraturan : - PK 2 Lampiran 2.0 : Kontrak Pusat Perolehan Perisian, Perkhidmatan Dan Perkakasan Microsoft Di Bawah Master Licensing Agreement (MLA) 3.0	i. Adakah perisian Microsoft yang digunakan mempunyai lesen yang sah?	Semua perisian Microsoft berlesen yang digunakan hendaklah mempunyai lesen yang sah.	
			ii. Adakah dokumen lesen perisian disimpan dengan baik?	Lesen berbentuk *hardcopy* atau digital disimpan dengan selamat.	
2.	Pusat Data	Pengurusan dan kawalan keselamatan pusat data Peraturan : - Pekeliling Am Bil 3 Tahun 2000 : Rangka Dasar Keselamatan Teknologi Maklumat Dan Komunikasi Kerajaan - Garis Panduan MAMPU: *Electronic Government Activities Act 2007* - Garis Panduan MAMPU: Arahan Teknologi Maklumat Disember 2007 - Garis Panduan Penyimpanan dan Pemeliharaan Rekod Elektronik Sektor Awam - Akta Arkib Negara 2003, Bahagian IV Pengurusan Rekod	i. Adakah pusat data mempunyai kawalan keselamatan dan persekitaran yang baik?	Pusat data mempunyai kawalan akses pintu, kamera litar tertutup(CCTV), kebakaran, susun atur kabel dan sistem penyejukan yang beroperasi dengan baik.	
			ii. Adakah pusat data mempunyai S*tandard Operating Procedure* (SOP)?	SOP pusat data disediakan.	
			iii. Adakah pusat data mempunyai rekod pegawai keluar masuk?	Rekod keluar masuk manual/elektronik disediakan.	
			iv. Adakah data dibuat *backup* berjadual?	Backup berjadual secara berkala, harian, mingguan, bulanan dan tahunan.	
			v. Adakah *tape backup* disimpan di lokasi lain (*Disaster Recovery)*?	Tape backup disimpan di luar kawasan pejabat	
			vi. Adakah ujian *restoration backup* dibuat secara berjadual?	Jadual restoration backup disediakan secara berkala	
			vii. Adakah perkakasan mempunyai penyenggaraan berjadual (*preventive maintenance*)?	Semua perkakasan ICT mempunyai jadual PM.	

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
3.	Pelan Kesinambungan Perkhidmatan	Peraturan : - Surat KP MAMPU 22 Januari 2010 :Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam	i. Adakah agensi merancang dan menyediakan bajet bagi melaksanakan PKP agensi?	Penyediaan bajet PKP.	
			ii. Adakah PKP agensi disediakan?	PKP boleh disediakan secara dalaman atau secara *outsource.*	
			iii.Pengurusan Atasan agensi melantik Peneraju pelaksanaan PKP dan meluluskan penubuhan Pasukan PKP?	Pasukan ditubuhkan dan peneraju dilantik.	
			iv. Adakah proses, peranan dan tanggungjawab ahli pasukan ditentukan dan latihan diberi untuk melaksanakan tugas?	Tugas pasukan dan tanggungjawab ahli ditetapkan.	
			v. Adakah Sesi pendedahan PKP kepada Pengurusan Atasan sekali setahun atau apabila berlaku perubahan Pengurusan Atasan diadakan oleh Koordinator PKP?	Sesi pendedahan dilaksanakan oleh Koordinator PKP sekurang-kurangnya sekali setahun kepada pengurusan.	
			vi. Adakah terma rujukan program PKP diluluskan oleh Jawatankuasa Pemandu PKP?	TOR PKP diluluskan oleh Jawatankuasa Pemandu PKP.	
			vii. Adakah status kemajuan pelaksanaan program PKP dilaporkan dalam mesyuarat Pengurusan Atasan?	Mesyuarat membincangkan kemajuan program PKP.	

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
4.	Rangkaian	Pengurusan rangkaian dan keselamatan rangkaian dikawal dengan baik. Peraturan : - The Malaysian Public Sector ICT Management Security Handbook (MyMIS), 2002 - Surat Arahan Ketua Setiausaha Negara bertarikh 20 Oktober 2006: Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) Di Agensi-Agensi Kerajaan - Garis Panduan MAMPU: *Standard, Policies and Guidelines- Channels Framework Version* 1.0, Ogos 2003	i. Adakah *Network Topology* dikemas kini?	*Network toplogy* hendaklah menunjukkan LAN, WAN, VPN, Firewall, Zon dan subnetting.	
			ii. Adakah keperluan perkakasan mencukupi bagi semua pegawai yang dirangkaikan?	Keperluan perkakasan mencukupi berdasarkan keperluan pegawai melaksanakan tugas.	
			iii. Adakah *SOP* rangkaian dan infrastruktur ICT disediakan?	SOP rangkaian dan infrastruktur disediakan.	
			iv. Adakah agensi melaksanakan langkah-langkah pengukuhan ke atas sistem rangkaian tanpa wayar.	Pengukuhan sistem rangkaian tanpa wayar menggunakan kaedah enkripsi dan *network key* yang kukuh, kerap menukar kata laluan atau *network key* serta kawalan penggunaan *MAC Address*.	
5.	Keselamatan	Menjelaskan mekanisme pelaporan insiden keselamatan teknologi maklumat dan komunikasi ICT. Peraturan : - Garis Panduan MAMPU: Garis Panduan Pengurusan Keselamatan ICT Sektor Awam Malaysia (*MyMis*)(MAMPU 2000)	i. Adakah agensi melaksanakan penilaian risiko	Penilaian risiko dilaksanakan sekurang-kurang sekali setahun atau sekiranya terdapat perubahan	
			ii. Adakah agensi melaksanakan penilaian tahap keselamatan rangkaian dan sistem ICT	Penilaian tahap keselamatan rangkaian dan sistem ICT dilaksanakan sekurang-kurang sekali setahun.	
			iii. Adakah Laporan pengukuhan dibentangkan di JPICT Jabatan.	Laporan Pengukuhan dibentangkan di JPICT Jabatan.	

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
		- Surat Pekeliling Am Bil.3 Tahun 2009 Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam - Surat Pekeliling Am Bil. 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam - Surat Pekeliling Am Bil. 4 Tahun 2006 : Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (Ict) Sektor Awam - Pekeliling Am Bil.1 Tahun 2001 : Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT) - Surat Arahan Ketua Pengarah MKN Berkaitan Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (GCERT) Oleh Agensi Keselamatan Siber Negara (NACSA) (28 Januari 2019) - Pekeliling Am Bil. 3 Tahun 2000 : Rangka Dasar Keselamatan Teknologi Maklumat Dan Komunikasi Kerajaan	iv. Adakah pasukan pengendali insiden (CERT) ditubuhkan?	Pasukan CERT ditubuhkan berdasarkan salah satu model CERT yang ditetapkan.	
			v. Adakah Insiden keselamatan dilaporkan sewajarnya?	Insiden keselamatan dilaporkan dan difailkan.	

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
		- Surat Arahan Ketua Pengarah MAMPU Berkaitan Pengaktifan Fail Log Server.(Rujukan : MAMPU.702-1/1/7 Jld.3(48) bertarikh 23 Mac 2009)	vi. Adakah fail log server dan aplikasi diaktifkan?	Fail log yang perlu diaktifkan adalah: • Fail log sistem pengoperasian • Fail log servis (cth:web, ftp, mel dll) • Fail log aplikasi (audit trail) • Fail log rangkaian (switch, firewall, router, IDS/IPS dll.)	
6.	Internet dan e-mail	Pengurusan Internet dan E-mel dilaksanakan dan dikawal penggunaannya dengan baik. Peraturan : - Pekeliling Kemajuan Pentadbiran Awam Bil.1 Tahun 2003 : Garis Panduan Mengenai Tatacara Penggunaan Internet Dan Mel Elektronik Di Agensi- agensi Kerajaan - Surat Arahan Ketua Pengarah MAMPU:Penggunaan Media Jaringan Sosial Di Sektor Awam (19 Nov. 2009) - Pekeliling Am Bil.3 Tahun 2000 : Rangka Dasar Keselamatan Teknologi Maklumat Dan Komunikasi Kerajaan (ICT) - Dasar Keselamatan ICT(DKICT) 24 Mei 2010 Versi 5.3	i. Adakah pentadbir sistem dilantik bagi menguruskan kawalan akses Internet dan e-mel?	Pentadbir Sistem ICT bertanggungjawab menguruskan kawalan akses internet dan e-mel	
			ii. Adakah pentadbir sistem ICT menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan Ketua Jabatan.	Pentadbir Sistem ICT agensi menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan Ketua Jabatan.	
			iii. Adakah terdapat kawalan akses semasa penggunaan Internet dan e-mel kepada sensitiviti maklumat (eg. pornografi) diberi perhatian?	Senarai sekatan akses penggunaan internet terhadap maklumat sensitif disedia dan dikemaskinikan.	
			iv. Adakah program-program kesedaran keselamatan ICT diberikan kepada semua pengguna agar penggunaan Internet dan e-mel dapat dilaksanakan dengan cara yang betul dan selamat.	Program Keselamatan ICT telah dihebahkan kepada semua pegawai menggunakan salah satu medium hebahan.	

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
7.	Laman Web	Pengurusan Laman Web mengikut peraturan pekeliling. Peraturan : - Pekeliling Kemajuan Pentadbiran Awam Bil. 2 Tahun 2015: "Pengurusan Laman Agensi Sektor Awam" - Surat Arahan Ketua Pengarah MAMPU:Panduan Penyediaan Berita *Online* dan Penyiaran Berita *Online* Di Laman Web/Portal Agensi-Agensi Kerajaan - (11 September 2009)	i. Adakah perkhidmatan dan maklumat agensi yang bersesuaian boleh dicapai melalui myGovernment ?	Laman web agensi boleh dicapai melalui laman web myGovernment.	
			ii. Adakah struktur tadbir urus laman web/portal di agensi diwujudkan ?	Jawatankuasa tadbir urus laman web diwujudkan.	
			iii. Adakah laman web yang dibangunkan mematuhi prinsip dan ciri-ciri asas	Mematuhi kesemua ciri-ciri asas mandatori	
			iv. Adakah agensi melaksanakan tugas-tugas penyenggaraan laman web/portal	1. Menyenggara server dan memastikannya berfungsi dengan baik 2. Menyemak dan memperbaiki broken links. Terdapat perisian yang boleh menyemak broken links bagi laman web/portal. Contoh perisian adalah WebExact yang boleh dicapai di alamat berikut: http://webxact.watchfire.com 3. Membetulkan kesilapan dan mengemaskini maklumat 4. Memaparkan maklumat terkini. Contoh: pekeliling baru, dasar baru dan sebagainya. 5. Menambah kandungan baru. 6. Menambahbaik susun atur, gambar dan grafik. 7. Mengurus pangkalan data laman web/portal.	

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
			v. Adakah penyediaan dan penyiaran berita *online* mematuhi garis panduan dan menggunakan teknologi *Really Simple Syndicate* (RSS)?	Penyiaran berita online disediakan mengikut peraturan dan menggunakan RSS.	
			vi. Adakah langkah-langkah keselamatan laman web/portal agensi dilaksanakan?	Semua ukuran pematuhan di bawah mestilah dipatuhi untuk dikira sebagai Patuh. Ciri-ciri keselamatan laman web dilaksanakan di mana berkaitan adalah: 1. Membezakan kategori maklumat umum dan maklumat dilindungi 2. *Backup/Restore* - Menyimpan 3 generasi *backup* - Menyimpan *backup* di lokasi berlainan 3. Penduaan 4. Kawalan keselamatan secara pentadbiran - Dasar/Standard/ Prosedur /Garis Panduan 5. Kawalan Keselamatan Logikal/Teknikal - *Firewall Intrusion Prevention System, Intrusion Detection*	

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
				6. Kawalan Keselamatan Fizikal - Kawalan keselamatan rangkaian, aplikasi, *patching*, pengasingan tugas pelayan web, pengauditan dan AWRS 7. Pengesahan kuasa *(authorization)* 8. Pengesahan capaian *(authentication)* - Penggunaan ID/Kata laluan - Penggunaan sijil digital/token 9. *Encryption* 10. Protokol rangkaian keselamatan - *Secure Socket Layer* 11. Penamatan sesi.	

Nota :

T.B.	-	Tidak Berkenaan
ICT	-	*Information Communication Technology*
SOP	-	*Standard Operating Procedure*
CIO	-	*Chief Information Officer*
SMS	-	*Short Message Service*