DASAR KESELAMATAN ICT versi 4.0

Pejabat Setiausaha Kerajan Negeri Selangor

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
23 Februari 2024	4.0	JPICT Bil. 1/2024	1 Julai 2024
23 April 2019	3.0	JPICT Bil. 4/2019	20 Jun 2019
30 September 2015	2.0	JPICT Bil. 4/2015	1 November 2015
29 April 2014	1.2	JPICT Bil. 2/2014	18 Ogos 2014
23 Januari 2013	1.1	JPICT Bil. 1/2013	05 Februari 2013
04 Oktober 2010	1.0	JPICT Bil. 4/2010	12 November 2010

JADUAL PINDAAN

TARIKH	VERSI	BUTIRAN PINDAAN
30 Sept 2015	**2.0**	1. Pindaan keseluruhan bagi memenuhi keperluan standard ISO/IEC 27001:2013 Information Security Management System (ISMS)
20 Jun 2019	**3.0**	1. Pindaan nama Bahagian Teknologi Maklumat (BTM) kepada Bahagian Pengurusan Maklumat (BPM). 2. Pindaan nama unit Keselamatan Rangkaian (KnR) kepada Pusat Data, Rangkaian Keselamatan (PDRK). 3. Pindaan nama unit Khidmat Sokongan (KS) kepada Unit Operasi dan Sokongan Teknikal (OST). 4. Pindaan nama perkakasan ICT kepada Aset ICT. 5. Pindaan kepada 020104 Pegawai Keselamatan ICT (ICTSO): Jawatan ICTSO disandang oleh Ketua Penolong Setiausaha (Operasi) 6. Mengemaskini pada bidang 020105 Pentadbir Sistem (f) Memantau aktiviti capaian system aplikasi pengguna. 7. Mengemaskini pada bidang 020107 Pentadbir Pengkalan Data (f) Memastikan kawalan capaian pengguna pengkalan data berdasarkan kepada DKICT. 8. Mengemaskini pada bidang 020108 Pentadbir Web (e) Mengenalpasti kandungan dan aplikasi atas talian sama ada untuk capaian secara Intranet dan Internet 9. Penambahan bidang 020109 Pentadbir Pusat Data. 10. Penambahan bidang 020110 Pentadbir E-mel. 11. Penambahan bidang 020112 Jawatankuasa Teknikal ICT PEJABAT SUK SELANGOR (JTICT) 12. Mengemaskini pada bidang 020113 Jawatankuasa Pemandu ICT PEJABAT SUK SELANGOR (JPICT)

TARIKH	VERSI	BUTIRAN PINDAAN
20 Jun 2019	**3.0**	13. Pindaan pada bidang 040101 Aset ICT : (a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan aset bernilai rendah mengikut Tatacara Pengurusan Aset Alih yang sedang berkuatkuasa dan sentiasa dikemaskini. 14. Penambahan bidang 040202 Data Terbuka Negeri Selangor. 15. Mengemaskini bidang 050203 Pengurusan Kata Laluan: i) Kata laluan disarankan untuk ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; 16. Mengemaskini pada bidang 050302 Capaian Internet; 17. Penggunaan Internet hanyalah untuk kegunaan rasmi dan berkaitan dengan bidang kerja. Walaubagaimanapun, Ketua Jabatan boleh memberi kebenaran kepada pengguna untuk menggunakan internet bagi tujuan lain. 18. Penggunaan *modem/router* untuk tujuan sambungan ke Internet selain daripada yang disediakan oleh BPM tidak dibenarkan sama sekali; 19. Menyedia, memuat naik, memuat turun dan menyimpan material, teks, ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah dan apa-apa yang boleh mengancam ketenteraman awam. 20. Mengemaskini pada bidang 0504 Kawalan Capaian Sistem Pengoperasian : 21. Memansuhkan perkara (b) Merekodkan capaian yang Berjaya dan gagal. 22. Membekalkan kemudahan kata kunci untuk pengesahan. 23. Penambahan bidang 050502 Prosedur *Secure Log-on*. 24. Penambahan bidang 050603 *Bring Your Own Device*. 25. Mengemaskini 050601 Peralatan Mudah Alih. Peralatan mudah alih** hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan. **Laptop, notebook, tablet, dan lain-lain.

TARIKH	VERSI	BUTIRAN PINDAAN
20 Jun 2019	**3.0**	26. Mengemaskini bidang 050602 Kerja Luar Pejabat 27. Penambahan bidang 0507 Penggunaan Media Sosial. 28. Penambahan bidang 050701 Amalan Baik Pemaparan Media Sosial. 29. Penambahan bidang 050702 Panduan Umum Penggunaan Media Sosial. 30. Penambahan bidang 050703 Kawalan Keselamatan Penggunaan Media Sosial. 31. Penambahan bidang 050704 Penggunaan Peribadi Media Sosial. 32. Penambahan bidang 050705 Etika Penggunaan Media Sosial oleh Pegawai Awam. 33. Mengemaskini pada bidang 070101 Kawasan Larangan Lokasi ICT 34. (f) Pembekal yang dibawah masuk perlu diiringi oleh pegawai yang bertanggungjawab sehingga ke dalam Pusat Data. Sepanjang pembekal berada dalam Pusat Data, pemantauan adalah melalui CCTV. 35. Mengemaskini pada bidang 070201 Peralatan ICT: (m) Aset ICT yang hendak dibawa keluar dari premis PEJABAT SUK SELANGOR, perlulah mendapat kelulusan Pegawai Aset ICT atau Pegawai Aset Bahagian dan direkodkan bagi tujuan pemantauan; (n) Aset ICT yang hilang hendaklah dilaporkan kepada Ketua Jabatan dan Pegawai Aset ICT dengan segera; (o) Aset ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur kehilangan aset dalam Tatacara Pengurusan Aset yang sedang berkuatkuasa. 36. Mengemaskini pada bidang 070201 Peralatan ICT: Aset ICT yang hilang hendaklah dilaporkan kepada Ketua Jabatan/Bahagian/Seksyen dan Pegawai Aset ICT dengan segera; 37. Mengemaskini pada bidang 070204 Media Perisian Dan Aplikasi :

TARIKH	VERSI	BUTIRAN PINDAAN
20 Jun 2019	**3.0**	38. Mengemaskini pada bidang 070205 Pelupusan: • Pelupusan melibatkan semua aset ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau aset bernilai rendah yang dibekalkan oleh PEJABAT SUK SELANGOR dan ditempatkan di PEJABAT SUK SELANGOR dan Pejabat-pejabat Daerah Negeri Selangor. • (j) Pelupusan aset ICT adalah tertakluk kepada 1 Pekeliling Perbendaharaan (1PP) Pengurusan Aset bertajuk “Tatacara Pengurusan Aset Alih Kerajaan” atau pekeliling terbaharu yang berkuatkuasa. 39. Mengemaskini pada bidang 070206 Peyelenggaraan Perkakasan. (f) Bantuan teknikal/ aduan tentang masalah-masalah yang dihadapi dalam penggunaan ICT hendaklah dilaporkan melalui Sistem E-helpdesk (https://ehelpdesk.selangor.gov.my) atau Helpdesk Bahagian Pengurusan Maklumat (BPM) – 03-55447569. 40. Mengemaskini bidang 070207 Peralatan ICT yang dibawa keluar premis. 41. Mengemaskini pada bidang 070304 Prosedur Kecemasan. a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan PEJABAT SUK SELANGOR; 42. Penambahan bidang 0705 Kawalan Peralatan yang ditempatkan secara sementara/ Peralatan Sewaan / Peralatan Ujicuba (Proof of Concept). 43. Mengemaskini pada bidang 080102 Kawalan Perubahan. e) Setiap perubahan hendaklah dibuat dengan menggunakan Borang Pengurusan Perubahan 44. Penambahan bidang 080202 Penerimaan Sistem. Perkara -perkara yang perlu dipatuhi adalah seperti berikut : a) Semua sistem baru termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetuju.

TARIKH	VERSI	BUTIRAN PINDAAN
20 Jun 2019	**3.0**	b) Sebarang penyerahan atau penerimaan sistem baru perlu mendapat pengesahan/kelulusan pemilik sistem dan perlu melalui proses UAT *(User Acceptance Test*) dan FAT *(Final Acceptance Test*); dan c) Penyelenggaraan sistem tersebut adalah berdasarkan manual operasi dan prosedur yang ditetapkan. 45. Penambahan bidang 090101 Kawalan Infrastruktur Rangkaian. 46. Penambahan bidang 090101 Kawalan Infrastruktur Rangkaian: n) Semua capaian dari luar rangkaian PEJABAT SUK SELANGOR kepada sistem dalaman yang tidak boleh diakses dari luar, mestilah menggunakan *Virtual Private Network (VPN)* dan dikawal oleh BPM (PDRK); 47. Mengemaskini pada bidang 090203 Keselamatan Sistem Dokumentasi. 48. Mengemaskini pada bidang 100101 Keperluan Keselamatan Sistem Maklumat. • Mengeluarkan item C) di dalam bidang 100101. 49. Penambahan bidang 100104 Keselamatan Fail Sistem. 50. Penambahan bidang 100105 Keselamatan Perkhidmatan Aplikasi di Rangkaian Umum. 51. Pindaan pada bidang 120101 Mekanisme Pelaporan di bawah bidang 12 Pengurusan Pengendalian Insiden Keselamatan. 52. Pindaan pada bidang 120201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT. 53. Mengemaskini bidang 140104 Pelanggaran Perundangan seperti berikut : i) Memberi e-mel/surat teguran kepada pelaku dan satu Salinan emel akan turut diberi kepada Ketua Jabatan / pegawai pelaku. iv) Mengambil tindakan berupa menarik balik kemudahan capaian internet/ peralatan ICT/ komputer (sementara/kekal) bergantung kepada jenis dan tahap kesalahan. 54. Mengemaskini bidang 140103 Keperluan Perundangan pada Lampiran 3.

TARIKH	VERSI	BUTIRAN PINDAAN
23 Februari 2024	**4.0**	1. Pindaan nama YB Setiausaha Kerajaan Negeri (Y.B. SUK) kepada YB Setiausaha Kerajaan Negeri (YB SUK). 2. Pindaan Ketua Pegawai Digital (CDO) pada bidang: i) 010101 Pelaksanaan Dasar ii) 020102 Ketua Pegawai Maklumat 3. Pindaan nama Y.B. SUK kepada YB DATO SUK; 4. Mengemaskini pada bidang 020105 (i) menyediakan laporan mengenai aktiviti capaian secara berkala (jika perlu). 5. Penambahan pada bidang 020106 pentadbir rangkaian: (h) memastikan sebarang pengubahsuaian Pejabat yang melibatkan pendawaian rangkaian dalaman hendaklah dipantau. 6. Pindaan pada bidang 020110 Pentadbir Emel: (e) Memastikan pengguna e-mel SUK SELANGOR berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel SUK SELANGOR dan Internet SUK SELANGOR serta pelaksanaan program kesedaran melalui e-mel (Penggunaan E-mel dan Internet) secara berterusan. 7. Pindaan pada bidang 020112 Jawatankuasa Teknikal ICT (JTICT) Pejabat SUK Selangor. 8. Pindaan pada bidang 020113 Jawatankuasa Pemandu ICT (JPICT) Pejabat SUK Selangor. 9. Pindaan pada bidang 020114 Jawatankuasa Tindak Balas Insiden Keselamatan ICT Pejabat SUK Selangor (SUK CSIRT Selangor). 10. Penambahan pada bidang 030104 Bertukar atau Tamat Perkhidmatan: (c) sebarang pertukaran pegawai hendaklah dimaklumkan kepada jabatan berkaitan: Contoh: akaun e-mel kepada BPM

TARIKH	VERSI	BUTIRAN PINDAAN
23 Februari 2024	**4.0**	11. Pindaan pada bidang 040101 Aset ICT i) a) Tatacara Pengurusan Aset Alih tukar kepada Tatacara Pengurusan Aset Alih Kerajaan ii) f) Pegawai Aset ICT tukar kepada Penyelaras Aset (BPM): • Bidang 040101 Aset ICT • Bidang 070201 Peralatan ICT (l-r) • Bidang 070205 Pelupusan • Butiran pindaan (34&35) 12. Mengemaskini pada bidang 040201 Pengelasan Maklumat 13. Pindaan pada bidang 040203 Pengendalian Maklumat daripada JPICT tukarkan kepada ICTSO (kiv) 14. Pindaan pada bidang 050101 Keperluan Kawalan Capaian daripada BPM Pejabat SUK Selangor; SUB (BPM); ICTSO tukarkan kepada Pejabat SUK Selangor; SUB (BPM); ICTSO 15. Mengemaskini pada bidang 050203 Pengurusan Kata Laluan. 16. Mengemaskini pengelasan “semua” kepada “semua kakitangan SUK dan PDT” pada bidang: i) 050204 *Clear Desk* dan *Clear Screen.* ii) 110101 Keperluan Keselamatan Kontrak dengan Pihak Ketiga iii) 110201 Kawalan Keselamatan Maklumat Melalui Perjanjian dengan Pembekal iv) 140101 Pematuhan Dasar 17. Mengemaskini pada bidang 050302 Capaian internet: a) Penggunaan internet di PEJABAT SUK SELANGOR hendaklah dipantau secara berterusan oleh BPM bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code, virus, ransomware* dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian PEJABAT SUK SELANGOR;

TARIKH	VERSI	BUTIRAN PINDAAN
23 Februari 2024	**4.0**	g) Penggunaan Internet hanyalah untuk kegunaan rasmi dan berkaitan dengan bidang kerja. Permohonan penggunaan internet bagi tujuan selain kegunaan rasmi hendaklah melalui Ketua Jabatan dan diluluskan oleh Pengurus ICT / ICTSO / Ketua Unit (KnR) l) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board.* Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan CDO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; 18. Mengemaskini ayat pada bidang 050501 Capaian Aplikasi dan Maklumat: d) Disarankan untuk menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; 19. Mengemaskini ayat pada bidang 050502 *Prosedur Secure Log-on:* d) Perlindungan terhadap *Brute Force log-on* adalah disarankan. (contoh: penggunaan captcha atau setaraf) 20. Penambahan pada bidang 050601 Peralatan Mudah Alih: b) Memastikan peralatan mudah alih yang dibawa keluar dari pejabat perlu disimpan dan dijaga dengan baik bagi mengelakkan daripada kecurian. 21. Mengemaskini pada bidang 060101 Enkripsi 22. Mengemaskini pada bidang 070201 Peralatan ICT: o) Aset ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur kehilangan aset dalam Tatacara Pengurusan Aset Alih Kerajaan yang sedang berkuatkuasa. y) Memastikan plag dicabut daripada suis utama *(Main Switch)* bagi mengelakkan kerosakan perkakasan (selain daripada perkakasan pusat data) sebelum meninggalkan pejabat terutama pada musim perayaan yang panjang bagi mengelakkan sebarang bencana berlaku.

TARIKH	VERSI	BUTIRAN PINDAAN
23 Februari 2024	**4.0**	23. Mengemaskini pada bidang 070204 Media Perisian dan Aplikasi: a) Perisian-perisian ICT yang disokong oleh BPM untuk pemasangan, penyelenggaraan dan latihan adalah termasuk: i. MS Office yang terdiri daripada: • MS Word • MS Excel • MS Powerpoint • MS Outlook / Outlook Web Access (OWA) ii. Web Browser iii. Acrobat Reader iv. WinZip / File Compress v. Antivirus vi. Dewan Eja vii. Sistem kewangan Kerajaan viii. Software Cleaning 24. Mengemaskini pada bidang 0704 Keselamatan Dokumen: f) Pelupusan dokumen hendaklah mengikut Prosedur Keselamatan semasa seperti mana Arahan Keselamatan (Semakan dan pindaan 2017), Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan g) Menggunakan penyulitan *(encryption)* ke atas dokumen rahsia rasmi yang disediakan bertaraf sulit dan terhad sahaja boleh disimpan dan dihantar secara elektronik. 25. Mengemaskini pada bidang 080102 Kawalan Perubahan: e) Setiap perubahan hendaklah direkodkan 26. Penambahan pada bidang 080103 Pengasingan Tugas dan Tanggungjawab: d) Pemilik sistem hendaklah bertanggungjawab sepenuhnya ke atas Pengurusan Pengasingan Tugas dan Tanggungjawab kakitangan dan pembekal

TARIKH	VERSI	BUTIRAN PINDAAN
23 Februari 2024	**4.0**	27. Mengemaskini pada bidang 080202 Penerimaan Sistem: c) Sebarang penyerahan atau penerimaan sistem baru perlu mendapat pengesahan/kelulusan pemilik sistem dan perlu melalui proses FAT (Final Acceptance Test); dan 28. Mengemaskini pada bidang 080401 Backup: d) Backup hendaklah dilaksanakan secara harian, mingguan, bulanan dan/atau tahunan. Kekerapan backup bergantung pada tahap kritikal maklumat; 29. Mengemaskini 090101 Kawalan Infrastruktur Rangkaian: f) Semua capaian kepada Internet dan sistem aplikasi mestilah melalui firewall dan dikawal oleh BPM; 30. Mengemaskini pada bidang 090302 Pengurusan Mel Elektronik (E-mel): y) Akaun e-mel pengguna yang tidak aktif antara 30 hingga 90 hari akan dibekukan penggunaannya dan seterusnya dihapuskan selepas 30 hari kecuali dimaklumkan kepada Pentadbir E-mel. 31. Penambahan pada bidang 120101 Mekanisme Pelaporan c) Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan Pengendalian Insiden Keselamatan Siber Sektor Awam 32. Mengemaskini pada bidang 130101 Pelan Pengurusan Kesinambungan Perkhidmatan e) Melaksanakan simulasi pelan sekurang-kurangnya mengikut kepada PKP; 33. Penambahan pada bidang 130102 Pelan Pengurusan Pemulihan Bencana *(Disaster Recovery Plan):* a) Mengenal pasti berdasarkan BCP pejabat alternatif dan/atau f) Melaksanakan pengujian dan latihan kepada kakitangan apabila perlu;

ISI KANDUNGAN

PENGENALAN

Pejabat Setiausaha Kerajaan Negeri Selangor (PEJABAT SUK SELANGOR) berperanan untuk menyediakan perkhidmatan bagi perancangan, pembangunan dan pengurusan sumber manusia sektor awam yang cemerlang berteraskan profesionalisme, integriti dan teknologi. Dokumen ini menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dan melindungi aset ICT Pejabat SUK Selangor. Dokumen ini diguna pakai oleh semua pihak kakitangan, pengguna dan pembekal yang menyediakan perkhidmatan, mencapai dan menggunakan aset dan sistem aplikasi ICT di PEJABAT SUK Selangor.

OBJEKTIF

Dasar Keselamatan ICT (DKICT) SUK Selangor diwujudkan untuk menjamin kesinambungan urusan SUK Selangor dengan meminimumkan kesan insiden keselamatan ICT.

Dasar ini juga sesuai untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi SUK Selangor. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Manakala, objektif utama DKICT di PEJABAT SUK SELANGOR adalah seperti berikut:

1) Memastikan kelancaran operasi jabatan yang berlandaskan ICT dengan mencegah serta meminimumkan kerosakan atau kemusnahan aset ICT jabatan;
2) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan maklumat dan komunikasi (*CIA*^{3});
3) Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;
4) Meningkatkan tahap kesedaran keselamatan ICT kepada para kakitangan, pengguna dan pembekal;
5) Memperkemaskan pengurusan risiko;
6) Mencegah penyalahgunaan atau kecurian aset ICT PEJABAT SUK SELANGOR; dan
7) Melindungi aset ICT daripada penyelewengan oleh kakitangan, pengguna dan pembekal.

PENYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Keselamatan ICT adalah bermaksud keadaan dimana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Terdapat empat (4) komponen asas keselamatan ICT, iaitu:

1) Melindungi maklumat rahsia rasmi dan maklumat rasmi PEJABAT SUK SELANGOR dari capaian tanpa kuasa yang sah;
2) Menjamin setiap maklumat adalah tepat dan sempurna;
3) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
4) Memastikan akses hanya kepada pengguna-pengguna yang sah atau penerimaan maklumat dari sumber-sumber yang sah.

DKICT PEJABAT SUK SELANGOR merangkumi perlindungan ke atas semua bentuk maklumat elektronik dan/atau kertas bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

1) **Kerahsiaan** – maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan akses tanpa kebenaran;
2) **Integriti** – Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;
3) **Tidak boleh disangkal** – Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
4) **Kesahihan** – Data dan maklumat hendaklah dijamin kesahihannya; dan
5) **Ketersediaan** – Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT; ancaman yang wujud akibat daripada kelemahan tersebut; risiko yang mungkin timbul; dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

SKOP

Aset ICT PEJABAT SUK SELANGOR terdiri daripada organisasi, manusia, perisian, perkakasan, telekomunikasi, kemudahan ICT, perkhidmatan dan data. DKICT PEJABAT SUK SELANGOR telah menetapkan keperluan-keperluan asas keselamatan seperti berikut:

1) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan dengan cara yang boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan
2) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan PEJABAT SUK SELANGOR, perkhidmatan dan masyarakat.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, DKICT PEJABAT SUK SELANGOR ini merangkumi perlindungan ke atas semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

1. **Perkakasan**

   Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan PEJABAT SUK SELANGOR. Contoh peralatan dan periferal seperti komputer, pelayan, *firewall,* pencetak, peralatan media, peralatan komunikasi dan alat-alat prasarana seperti *Uninterruptible Power Supply (UPS)* dan sebagainya;

2. **Perisian**

   Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada PEJABAT SUK SELANGOR;

3. Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:

i) Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;

ii) Sistem halangan akses seperti sistem kad akses; dan

iii) Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

4. Data dan maklumat

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif PEJABAT SUK SELANGOR. Contohnya sistem dokumentasi, prosedur operasi, rekod-rekod PEJABAT SUK SELANGOR, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain;

5. Manusia

Semua pengguna infrastruktur ICT PEJABAT SUK SELANGOR yang dibenarkan, termasuk kakitangan, pengguna dan pembekal. Individu yang mempunyai pengetahuan untuk melaksanakan skop kerja harian PEJABAT SUK SELANGOR bagi mencapai misi dan objektif jabatan. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan;

6. Media storan

Semua media storan dan peralatan yang berkaitan seperti disket, storan mudah alih, kartrij, CD-ROM, pita, cakera, pemacu cakera, pemacu pita dan lain-lain;

7. Media komunikasi

Semua peralatan berkaitan komunikasi seperti pelayan rangkaian, *gateway, bridge, router*, peralatan PABX, *wireless* LAN, talian ISDN, peralatan *video conferencing, modem*, PCMCIA, kabel rangkaian, NIC, *switches, hub* dan lain-lain;

8. Dokumentasi

Semua dokumen (prosedur dan manual pengguna) yang berkaitan dengan aset ICT, pemasangan dan pengoperasian peralatan dan perisian, sama ada dalam bentuk elektronik atau bukan elektronik.

9. Premis Komputer dan Komunikasi

Semua kemudahan serta premis yang diguna untuk menempatkan perkara 1 hingga 8 di atas. Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

PRINSIP - PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT PEJABAT SUK SELANGOR dan perlu dipatuhi adalah seperti berikut:

1. Akses Atas Dasar Perlu Mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen **Arahan Keselamatan perenggan 53, muka surat 15;**

2. Hak Akses Minimum

Hak akses kepada pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah dan/atau menghapuskan/membatalkan sesuatu data atau maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

3. Kebertanggungjawaban/Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Bagi menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesahkan bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

ii) Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;

iii) Menentukan maklumat sedia untuk digunakan;

iv) Menjaga kerahsiaan kata laluan;

v) Mematuhi *standard*, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

vi) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

vii) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

4. Pengasingan

Tugas mewujud, menghapus, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan (*unauthorized access*) serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

5. Pengauditan

Tujuan aktiviti ini ialah untuk mengenalpasti insiden berkaitan keselamatan aset ICT atau keadaan yang mengancam keselamatan aset ICT. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

Dengan itu, aset ICT seperti komputer, pelayan, *router, firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau Jejak audit (*audit trail)*. Semua log yang berkaitan dengan aset ICT perlu disimpan bagi tujuan jejak audit;

6. Pematuhan

DKICT PEJABAT SUK SELANGOR hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT;

7. Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian bagi meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan dan ketidakbolehcapaian. Pemulihan boleh dilakukan melalui proses penduaan (*backup*) dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan (BRP); dan

8. Saling Bergantungan

Setiap prinsip di atas adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu tindakan mempelbagaikan pendekatan dalam menyusun dan mencorak sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

PENILAIAN RISIKO KESELAMATAN ICT

PEJABAT SUK SELANGOR hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu PEJABAT SUK SELANGOR perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

PEJABAT SUK SELANGOR hendaklah melaksanakan penilaian risiko Keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat PEJABAT SUK SELANGOR termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses, prosedur serta kakitangan. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan yang lain.

PEJABAT SUK SELANGOR bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

PEJABAT SUK SELANGOR perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko yang berlaku dan memilih tindakan berikut:-

a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
b) Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;
c) Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
d) Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

BIDANG 01 DASAR KESELAMATAN (*A.5 Information security policies*)	
0101 Dasar Keselamatan ICT	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan PEJABAT SUK SELANGOR yang berkaitan.	
010101 Pelaksanaan Dasar	
Pelaksanaan dasar ini akan dijalankan oleh YB Setiausaha Kerajaan Negeri (YB DATO SUK) dibantu oleh Jawatankuasa Pemandu ICT PEJABAT SUK SELANGOR (JPICT) yang terdiri daripada :- i) Ketua Pegawai Digital (CDO) ii) Setiausaha Bahagian, SUB (BPM); iii) Pegawai Keselamatan ICT (ICTSO); iv) Semua Ketua Bahagian; dan v) Pegawai-pegawai yang diturunkan kuasa	YB DATO SUK CDO; SUB (BPM); ICTSO; Ketua Bahagian; Pegawai-pegawai yang diturunkan kuasa
010102 Penyebaran Dasar	
Dasar ini perlu disebarkan kepada semua pengguna yang terlibat dengan infrastruktur ICT PEJABAT SUK SELANGOR meliputi kakitangan, pengguna dan pembekal.	ICTSO
010103 Penyelenggaraan Dasar	
Dasar Keselamatan ICT PEJABAT SUK SELANGOR adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT PEJABAT SUK SELANGOR: a) Mengenal pasti dan menentukan perubahan yang diperlukan; b) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan, pertimbangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT), PEJABAT SUK SELANGOR; c) Memaklumkan perubahan yang telah dipersetujui oleh JPICT kepada semua pihak iaitu kakitangan, pengguna dan pembekal; dan d) Menyemak semula dokumen pada jangka masa yang dirancang atau mengikut keperluan dan perubahan ketara bagi memastikan dokumen sentiasa relevan dan berkesan.	JPICT; ICTSO
010104 Pengecualian Dasar	
Dasar Keselamatan ICT PEJABAT SUK SELANGOR adalah terpakai dan mestilah dipatuhi oleh semua kakitangan, pengguna serta pembekal ICT PEJABAT SUK SELANGOR dan tiada pengecualian diberikan.	Semua

BIDANG 02
ORGANISASI KESELAMATAN *(A.6 Organization of information security)*

0201 Infrastruktur Organisasi Dalaman

Objektif:
Menerangkan peranan dan tanggungjawab semua pihak yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT PEJABAT SUK SELANGOR.

020101 YB Setiausaha Kerajaan Negeri (YB DATO SUK)	
Peranan dan tanggungjawab YB DATO SUK adalah seperti berikut: i) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT PEJABAT SUK SELANGOR; ii) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT PEJABAT SUK SELANGOR, iii) Memastikan semua keperluan jabatan seperti sumber kewangan, sumber kakitangan dan perlindungan keselamatan adalah mencukupi, dan iv) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT PEJABAT SUK SELANGOR;	YB DATO SUK
020102 Ketua Pegawai Digital (CDO)	
Ketua Pegawai Digital (CDO) adalah disandang oleh Timbalan Setiausaha Kerajaan Negeri (Pengurusan). CDO bertangggungjawab ke atas perancangan, pengurusan, penyelarasan dan pemantauan program ICT di PEJABAT SUK SELANGOR.	CDO
020103 Pengurus ICT	
Jawatan Pengurus ICT adalah disandang oleh Setiausaha Bahagian Pengurusan Maklumat (SUB BPM). Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a) Memastikan DKICT PEJABAT SUK SELANGOR dilaksanakan di bahagian; b) Memastikan semua kakitangan, perunding, kontraktor dan pembekal yang terlibat dengan bahagian mematuhi dasar, piawaian dan garis panduan keselamatan ICT dan seterusnya melaporkan sebarang insiden berkaitan keselamatan ICT; c) Mengkaji semula aspek-aspek keselamatan fizikal seperti kemudahan *backup* dan persekitaran pejabat yang perlu; d) Melaksanakan keperluan DKICT dalam operasi semasa seperti berikut: i) Pelaksanaan sistem atau aplikasi baru sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baru; ii) Pembelian atau peningkatan perisian dan sistem komputer; iii) Perolehan teknologi dan perkhidmatan komunikasi baru; dan iv) Pelantikan pembekal, perunding atau rakan usaha sama.	SUB (BPM)

BIDANG 02 ORGANISASI KESELAMATAN (A.6 Organization of information security)	
e) Menyimpan rekod atau laporan terkini tentang ancaman keselamatan. Sebarang perkara atau penemuan ancaman terhadap keselamatan ICT hendaklah dilaporkan kepada ICTSO; f) Membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam jabatan yang mematuhi keperluan DKICT PEJABAT SUK SELANGOR; g) Membangun, mengkaji semula dan mengemas kini pelan kontingensi keselamatan ICT di bahagian; h) Melaksanakan sistem kawalan capaian pengguna ke atas aset-aset ICT PEJABAT SUK SELANGOR; i) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan PEJABAT SUK SELANGOR; j) Menentukan kawalan akses pengguna terhadap aset ICT PEJABAT SUK SELANGOR; k) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; l) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT PEJABAT SUK SELANGOR.	
020104 Pegawai Keselamatan ICT (ICTSO)	
Jawatan Pegawai Keselamatan ICT (ICTSO) adalah disandang oleh Ketua Penolong Setiausaha (Operasi). Peranan dan tanggungjawab ICTSO adalah seperti berikut: a) Mengurus keseluruhan program keselamatan ICT PEJABAT SUK SELANGOR; b) Memberi penerangan dan pendedahan berkenaan DKICT PEJABAT SUK SELANGOR kepada semua pengguna; c) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT PEJABAT SUK SELANGOR. d) Menjalankan pengurusan risiko; e) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan PEJABAT SUK SELANGOR berdasarkan hasil penemuan dan menyediakan laporan mengenainya; f) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; g) Mencadangkan langkah-langkah pengukuhan bagi mematuhi dasar-dasar berkaitan keselamatan ICT PEJABAT SUK SELANGOR; h) Melaporkan insiden keselamatan ICT kepada pihak NACSA dan seterusnya membantu dalam penyiasatan atau pemulihan; i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; j) Menjalankan program-program kesedaran mengenai keselamatan ICT;	ICTSO

BIDANG 02 ORGANISASI KESELAMATAN (*A.6 Organization of information security*)	
k) Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlaku ancaman kepada keselamatan ICT dan menyediakan khidmat nasihat serta langkah pemulihan yang bersesuaian; l) Memastikan pematuhan DKICT PEJABAT SUK SELANGOR oleh pihak luaran seperti perunding, kontraktor dan pembekal yang mencapai dan menggunakan aset ICT PEJABAT SUK SELANGOR untuk tujuan penyelenggaraan, pemasangan, naik taraf dan sebagainya; m) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan ICT; n) Memastikan DKICT PEJABAT SUK SELANGOR dikemas kini sesuai dengan perubahan teknologi, arahan jabatan dan ancaman-ancaman dari semasa ke semasa; dan o) Memastikan Pelan Strategik ICT PEJABAT SUK SELANGOR mengandungi aspek keselamatan ICT.	
020105 Pentadbir Sistem	
Peranan dan tanggungjawab Pentadbir Sistem adalah seperti berikut: a) Memastikan ketepatan dan menyekat kebenaran capaian serta- merta apabila tidak lagi diperlukan atau melanggar DKICT PEJABAT SUK SELANGOR; b) Melaksanakan prinsip-prinsip DKICT dan menjaga kerahsiaan maklumat PEJABAT SUK SELANGOR; c) Menentukan ketepatan dan kesempurnaan kawalan capaian pengguna berdasarkan kepada garis panduan keselamatan ICT PEJABAT SUK SELANGOR; d) Mengambil tindakan segera dan bersesuaian apabila dimaklumkan oleh bahagian sekiranya terdapat pegawai yang telah tamat perkhidmatan, bertukar, berkursus panjang atau berlaku perubahan dalam bidang tugas; e) Memantau aktiviti pengguna yang diberi keutamaan capaian yang tinggi dan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT PEJABAT SUK SELANGOR; f) Memantau aktiviti capaian sistem aplikasi pengguna; g) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; h) Menganalisa dan menyimpan rekod jejak audit; i) Menyediakan laporan mengenai aktiviti capaian secara berkala; dan j) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	Pentadbir Sistem

BIDANG 02 ORGANISASI KESELAMATAN (*A.6 Organization of information security*)	
020106 Pentadbir Rangkaian	
Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut: a) Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di PEJABAT SUK SELANGOR beroperasi sepanjang masa; b) Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna; c) Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; d) Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; e) Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; f) Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian PEJABAT SUK SELANGOR secara tidak sah seperti melalui peralatan *modem* dan *dial-up;* g) Menyediakan akses khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian. h) Memastikan sebarang pengubahsuaian pejabat yang melibatkan pendawaian rangkaian dalaman hendaklah dipantau.	Pentadbir Rangkaian
020107 Pentadbir Pangkalan Data	
Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut: a) Melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data; b) Memastikan pangkalan data boleh digunakan pada setiap masa; c) Melaksanakan pemantauan dan penyenggaraan yang berterusan ke atas pangkalan data; d) Melaksanakan proses *backup* dan *restoration* ke atas pangkalan data; e) Memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur; f) Memastikan kawalan capaian pengguna pangkalan data berdasarkan kepada DKICT; g) Melaksanakan proses pembersihan data (*housekeeping*) di dalam pangkalan data; dan h) Melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.	Pentadbir Pangkalan Data

BIDANG 02 ORGANISASI KESELAMATAN *(A.6 Organization of information security)*	
020108 Pentadbir Web	
Peranan dan tanggungjawab Pentadbir Laman Web adalah seperti berikut: a) Memastikan kandungan laman web sentiasa sahih dan terkini; b) Memantau prestasi capaian dan menjalankan penilaian prestasi untuk memastikan akses yang lancar; c) Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman; d) Menghadkan capaian Pentadbir Laman Web Bahagian ke *web server*; e) Mengenalpasti kandungan dan aplikasi atas talian sama ada untuk capaian secara Intranet dan Internet. f) Memastikan data-data SULIT tidak boleh disalin atau dicetak oleh orang yang tidak berhak; g) Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; h) Melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di *web server*; i) Melaksanakan proses *backup* dan *restoration* secara berkala; dan j) Melaporkan sebarang pelanggaran keselamatan laman portal kepada ICTSO.	Pentadbir Web
020109 Pentadbir Pusat Data	
Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti berikut: a) Memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat; b) Memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data; c) Menjadual dan melaksanakan proses backup dan restoration ke atas pangkalan data dan sistem secara berkala; d) Menyediakan perancangan bencana mengikut prinsip Pengurusan Kesinambungan Perkhidmatan dalam DKICT; e) Melaksanakan prinsip-prinsip DKICT; dan f) Memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan.	Pentadbir Pusat Data

BIDANG 02 ORGANISASI KESELAMATAN (*A.6 Organization of information security*)	
020110 Pentadbir E-mel	
Peranan dan tanggungjawab Pentadbir Emel adalah seperti berikut: a) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; b) Pentadbir e-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib; c) Mengesah dan memaklumkan kepada ICTSO sekiranya mengalami insiden keselamatan melalui saluran rasmi; d) Memastikan kemudahan membuat capaian e-mel melalui pelbagai peralatan ICT dan alat komunikasi; dan e) Memastikan pengguna e-mel SUK SELANGOR berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel SUK SELANGOR dan Internet SUK SELANGOR serta pelaksanaan program kesedaran melalui e-mel (Penggunaan E-mel dan Internet) secara berterusan.	Pentadbir E-mel
020111 Pengguna	
Peranan dan tanggungjawab pengguna adalah seperti berikut: a) Pengguna warga PEJABAT SUK SELANGOR dan pihak ketiga perlu membaca, memahami dan mematuhi DKICT PEJABAT SUK SELANGOR; b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; d) Melaksanakan prinsip-prinsip DKICT dan menjaga kerahsiaan maklumat PEJABAT SUK SELANGOR; e) Melaksanakan langkah-langkah perlindungan seperti berikut: i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii) Menentukan maklumat sedia untuk digunakan; iv) Menjaga kerahsiaan kata laluan; v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan; vi) Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Pengguna

BIDANG 02 ORGANISASI KESELAMATAN *(A.6 Organization of information security)*	
viii) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; ix) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan x) Menandatangani Surat Akuan Pematuhan DKICT PEJABAT SUK SELANGOR sebagaimana **Lampiran 1**.	
020112 Jawatankuasa Teknikal ICT PEJABAT SUK SELANGOR (JTICT)	
Keanggotaan JTICT adalah seperti berikut: Pengerusi : SUB (BPM) Ahli : (1) ICTSO (2) Ketua Penolong Setiausaha Kanan (BPM) (3) Ketua Penolong Pengarah IT, Pejabat Tanah dan Galian Selangor (PTGS) (4) Penolong Pengarah IT, Jabatan Agama Islam Selangor (JAIS) (5) Pengarah IT, Majlis Bandaraya Shah Alam (6) Pengarah IT, Majlis Bandaraya Petaling Jaya (7) Pengarah IT, Majlis Perbandaran Subang Jaya (8) Pengarah IT, Majlis Perbandaran Selayang (9) Pengarah IT, Majlis Perbandaran Ampang Jaya (10) Penolong Pegawai Kewangan Negeri (IT), Perbendaharaan Negeri Selangor (11) PSU Kanan BPM (12) Ketua-Ketua Unit BPM Urusetia : BPM, PEJABAT SUK SELANGOR. Bidangkuasa : i) Memproses dan menilai semua permohonan perolehan projek ICT Kerajaan Negeri Selangor dan agensi Negeri di bawahnya; ii) Mengesyorkan perakuan teknikal projek ICT kepada JPICT Pejabat SUK Selangor; iii) Memantau kemajuan pembangunan dan pelaksanaan projek ICT agensi yang diluluskan oleh JPICT Pejabat SUK Selangor dan melaporkan kepada JPICT Pejabat SUK Selangor; iv) Mengenal pasti masalah dan isu semasa dalam pembangunan atau pelaksanaan projek ICT agensi di bawah Kerajaan Negeri Selangor serta mengesyorkan cadangan penyelesaian kepada JPICT Pejabat SUK Selangor; v) Menyediakan laporan kepada JPICT Pejabat SUK Selangor mengikut keperluan; dan vi) Meneroka teknologi baru dan terkini dalam memastikan arus pembangunan Projek-Projek ICT Kerajaan Negeri Selangor seiring dengan keperluan teknologi semasa.	JTICT

BIDANG 02
ORGANISASI KESELAMATAN *(A.6 Organization of information security)*

020113 Jawatankuasa Pemandu ICT PEJABAT SUK SELANGOR (JPICT)

Keanggotaan JPICT adalah seperti berikut:

Pengerusi : Timbalan Setiausaha Kerajaan Negeri Selangor (Pengurusan)

Ahli :
(1) Timbalan Pegawai Kewangan Negeri
(2) SUB (BPM)
(3) SUB (BKP)
(4) SUB (BPSM)
(5) SUB (Korporat)
(6) Ketua Audit Dalam
(7) Timbalan Pengarah Seksyen Agihan dan Pembangunan, UPEN
(8) Timbalan Pengarah Seksyen Makro dan Penswastaan, UPEN
(9) Penolong Pengarah IT, Jabatan Agama Islam Selangor (JAIS)
(10) KPSU (Kewangan), BKP
(11) Ketua Penolong Pengarah IT, Pejabat Tanah dan Galian Selangor (PTGS)
(12) Pengarah IT, Majlis Bandaraya Shah Alam
(13) Pengarah IT, Majlis Bandaraya Petaling Jaya
(14) Pengarah IT, Majlis Perbandaran Subang Jaya
(15) Pengarah IT, Majlis Perbandaran Selayang
(16) Pengarah IT, Majlis Perbandaran Ampang Jaya
(17) ICTSO
(18) Ketua Penolong Setiausaha Kanan (BPM)
(19) PSU Kanan BPM
(20) Ketua-Ketua Unit BPM

Urusetia : BPM, PEJABAT SUK SELANGOR.

Bidangkuasa :

i) Menetapkan arah tuju dan strategi untuk pembangunan dan pelaksanaan Projek-Projek ICT Kerajaan Negeri Selangor;

ii) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju/strategi ICT Kerajaan Negeri Selangor;

iii) Merancang dan menyelaras pembangunan program/projek ICT Kerajaan Negeri Selangor supaya selaras dengan Pelan Strategik Organisasi dan Pelan Strategik Teknologi Maklumat Kerajaan Negeri Selangor;

iv) Mempromosi dan menggalakkan perkongsian pintar projek ICT antara semua agensi di bawah Kerajaan Negeri Selangor;

v) Merancang dan menentukan langkah-langkah keselamatan ICT.

JPICT

BIDANG 02 ORGANISASI KESELAMATAN *(A.6 Organization of information security)*	
vi) Mengikuti dan memantau perkembangan program ICT agensi Kerajaan Negeri Selangor, serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pembangunan dan pelaksanaan ICT; vii) Menilai dan meluluskan semua perolehan ICT bagi Pejabat SUK dan agensi Kerajaan Negeri Selangor berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturanperaturan semasa yang berkaitan;	
020114 Pasukan Tindak Balas Insiden Keselamatan Siber ICT PEJABAT SUK SELANGOR (CSIRT) SUK SELANGOR	
Keanggotaan CSIRT SELANGOR adalah seperti berikut: **Pengarah** : SUB (BPM) **Pengurus** : KPSU / ICTSO **Ahli** : (1) KPSU Kanan (BPM); (2) PSU Kanan (BPM); (3) Semua PSU (BPM); (4) PPTM Kanan (BPM); (5) Semua PPTM (PDRK), BPM Selangor; (6) PPTM (OST), BPM Selangor; (7) Semua PPTM (Daerah) Selangor. (8) Jabatan-jabatan di bawah pentadbiran Kerajaan Negeri Selangor (Jabatan berkaitan); dan (9) ICTSO PBT Selangor. (10) Badan Berkanun Negeri **Urusetia** : BPM, PEJABAT SUK SELANGOR Peranan dan tanggungjawab CSIRT SELANGOR adalah seperti berikut: i) Memantau, mengesan insiden, menerima dan mengesahkan aduan insiden keselamatan siber, seterusnya mengenal pasti jenis insiden serta menilai impak insiden keselamatan siber ii) Merekod dan menjalankan siasatan awal terhadap insiden yang diterima. iii) Melaksanakan pengurusan dan pengendalian insiden keselamatan siber serta mengambil tindakan awal pemulihan.	CSIRT SELANGOR

BIDANG 02 ORGANISASI KESELAMATAN *(A.6 Organization of information security)*	
iv) Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan serta pengukuhan keselamatan siber supaya insiden Baharu dapat dielakkan. v) Melaporkan insiden keselamatan siber kepada agensi yang menyelianya (sekiranya ada) dan NC4. vi) Menasihat agensi di bawah selaiannya mengambil tindakan pemulihan dan pengukuhan. vii) Menyebarkan makluman/amaran berkaitan insiden kepada agensi lain di bawah seliaannya. viii) Memastikan fail log disimpan sekurang-kurangnya enam bulan di tempat yang selamat.	

BIDANG 03
KESELAMATAN SUMBER MANUSIA *(A.7 Human resources security)*

0301 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif :
Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan PEJABAT SUK SELANGOR, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga PEJABAT SUK SELANGOR hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.

030101 Sebelum Perkhidmatan

Memastikan pegawai dan kakitangan PEJABAT SUK SELANGOR, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, penipuan dan penyalahgunaan aset ICT. Perkara yang mesti dipatuhi termasuk yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan PEJABAT SUK SELANGOR, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan ke atas keselamatan ICT sebelum, semasa dan selepas perkhidmatan; b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan PEJABAT SUK SELANGOR c) Memenuhi keperluan prosedur keselamatan (NDA) bagi pembekal, pakar runding dan pihak-pihak lain yang berkepentingan selaras dengan keperluan perkhidmatan; dan d) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua

030102 Semasa Perkhidmatan

Memastikan pegawai dan kakitangan PEJABAT SUK SELANGOR, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong DKICT PEJABAT SUK SELANGOR dan meminimakan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara yang perlu dipatuhi termasuk yang berikut: a) Memastikan pegawai dan kakitangan PEJABAT SUK SELANGOR, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan ditetapkan PEJABAT SUK SELANGOR; b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pegawai dan kakitangan PEJABAT SUK SELANGOR secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa;	Semua

BIDANG 03 KESELAMATAN SUMBER MANUSIA (A.7 Human resources security)	
c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan PEJABAT SUK SELANGOR, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan yang ditetapkan PEJABAT SUK SELANGOR; dan d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Pengurusan Sumber Manusia (BPSM), PEJABAT SUK SELANGOR atau Bahagian Teknologi Maklumat Selangor.	
030103 Program Kesedaran Keselamatan ICT	
Setiap pengguna di PEJABAT SUK SELANGOR perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden juga adalah penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT PEJABAT SUK SELANGOR.	SUB (BPM)
030104 Bertukar Atau Tamat Perkhidmatan	
Memastikan pertukaran atau tamat perkhidmatan pegawai dan kakitangan PEJABAT SUK SELANGOR, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan diuruskan dengan teratur. Perkara yang perlu dipatuhi termasuk: a) Memastikan semua aset ICT dikembalikan kepada jabatan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b) Membatalkan atau meminda semua kebenaran capaian ke atas maklumat, kemudahan proses maklumat dan semua akses berkaitan mengikut peraturan yang ditetapkan PEJABAT SUK SELANGOR dan/atau terma perkhidmatan. c) Sebarang pertukaran pegawai hendaklah dimaklumkan kepada Jabatan berkaiatan : Contoh : akaun e-mel kepada BPM	SUB (BPSM); SUB (BPM) dan Ketua Jabatan

BIDANG 04
PENGURUSAN ASET (*A.8 Asset management*)

0401 Akauntabiliti Aset

Objektif :
Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset PEJABAT SUK SELANGOR.

040101 Aset ICT

Aset ICT terbahagi kepada dua kategori iaitu Harta Modal dan Aset Bernilai Rendah. Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Tanggungjawab yang perlu dipatuhi untuk memastikan semua aset ICT dikawal dan dilindungi: a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan borang daftar aset bernilai rendah mengikut Tatacara Pengurusan Aset Alih yang sedang berkuatkuasa dan sentiasa dikemaskini; b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c) Memastikan semua pengguna mengesahkan aset ICT yang ditempatkan di PEJABAT SUK SELANGOR; d) Semua peraturan pengendalian aset hendaklah dikenal pasti, didokumen dan dilaksanakan; e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya. f) Sebarang perlanggaran hendaklah dilaporkan kepada Pegawai Penyelaras Aset (BPM)	Pegawai Penyelaras Aset (BPM); Semua

0402 Pengelasan dan Pengendalian Maklumat

Objektif :
Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

040201 Pengelasan Maklumat

Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada PEJABAT SUK SELANGOR. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan (Semakan dan Pindaan 2017) seperti berikut: a) Rahsia Besar; b) Rahsia; c) Sulit; atau d) Terhad. e) Terbuka.	Semua

BIDANG 04 PENGURUSAN ASET (*A.8 Asset management*)	
040202 Data Terbuka Negeri Selangor	
Objektif : Objektif polisi ini adalah untuk memudahkan capaian kepada data dan maklumat milik Kerajaan yang boleh dikongsi dalam bentuk kebolehbacaan mesin dan kebolehbacaan manusia dengan cara yang proaktif dan seterusnya menggiatkan perkongsian data di kalangan agensi/jabatan. Perkongsian dan capaian akan dilaksanakan di dalam kerangka dasar-dasar, akta dan peraturan yang berkaitan, dengan itu membenarkan capaian dan penggunaan data dan maklumat Kerajaan secara lebih meluas melalui penerbitan data tebuka untuk kegunaan awam.	
Data terbuka merujuk data kerajaan yang boleh digunakan secara bebas, boleh dikongsikan dan digunakan semula oleh rakyat, agensi sektor awam atau swasta untuk sebarang tujuan. Pelaksanaan data terbuka dapat meningkatkan kualiti dan ketelusan penyampaian perkhidmatan kerajaan menerusi perkongsian data yang tepat, cepat dan relevan. Di samping itu, ia juga dapat meningkatkan produktiviti dan ekonomi negara melalui industri/inovasi baharu dengan penglibatan rakyat dan komuniti perniagaan. Data Terbuka adalah maklumat yang bebas digunakan, dikongsi dan digunakan semula oleh orang awam, agensi kerajaan dan organisasi swasta untuk pelbagai tujuan. Kementerian dan agensi hendaklah mematuhi pekeliling yang sedang berkuat kuasa.	Semua

BIDANG 04 PENGURUSAN ASET (A.8 Asset management)	
040203 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut: a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan; e) Mematuhi *standard*, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan; f) Melaksanakan peraturan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; g) Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum; h) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; i) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan j) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	JPICT; ICTSO

BIDANG 05 KAWALAN CAPAIAN *(A.9 Access control)*	
0501 Dasar Kawalan Capaian	
Objektif: Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT.	
050101 Keperluan Kawalan Capaian	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d) Kawalan ke atas kemudahan pemprosesan maklumat.	PEJABAT SUK SELANGOR; SUB (BPM); ICTSO;
0502 Pengurusan Capaian Pengguna	
Objektif: Mengawal capaian pengguna ke atas aset ICT PEJABAT SUK SELANGOR	
050201 Akaun Pengguna	
Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, Pentadbir Sistem perlu mengambil langkah-langkah berikut: a) Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; b) Akaun pengguna (*user id*) hendaklah unik dan mencerminkan identiti pengguna; c) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika kaedah penggunaannya melanggar peraturan; d) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; e) Pentadbir Sistem boleh menggantung dan menamatkan akaun pengguna atas sebab-sebab berikut: i) Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi tiga (3) bulan; ii) Bertukar bidang tugas kerja; iii) Bertukar ke agensi lain; iv) Bersara; atau v) Ditamatkan perkhidmatan	Pentadbir Sistem; Semua

BIDANG 05 KAWALAN CAPAIAN *(A.9 Access control)*	
050202 Hak Capaian (*Privilege*)	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem
050203 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh PEJABAT SUK SELANGOR seperti berikut: a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf dan nombor *(alphanumeric)* dan perlu mengandungi gabungan huruf besar dan kecil; d) Kata laluan hendaklah diingat dan tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama; f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g) Disarankan membuat pertukaran kata laluan semasa atau selepas login kali pertama, atau selepas kata laluan diset semula; h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i) Kata laluan disarankan untuk ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan j) Mengelakkan penggunaan semula kata laluan yang baru digunakan.	Pentadbir Sistem; Pengguna
050204 Clear Desk dan Clear Screen	
Prosedur *Clear Desk* dan *Clear Screen* perlu dipatuhi supaya maklumat dalam apa jua bentuk media disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* and *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Menggunakan kemudahan *password screen saver* atau *log out* apabila meninggalkan komputer;	Semua kakitangan SUK dan PDT

BIDANG 05 KAWALAN CAPAIAN *(A.9 Access control)*	
b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	
0503 Kawalan Capaian Rangkaian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
050301 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian PEJABAT SUK SELANGOR, rangkaian agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaiannya; dan c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pentadbir Rangkaian
050302 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Penggunaan internet di PEJABAT SUK SELANGOR hendaklah dipantau secara berterusan oleh BPM bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, *virus, ransomware* dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian PEJABAT SUK SELANGOR; b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; c) Penggunaan proksi (sekiranya ada) yang telah ditetapkan oleh PEJABAT SUK SELANGOR bagi mengawal akses Internet mengikut fungsi kerja dan mematuhi pekeliling semasa yang dikeluarkan; d) Penggunaan teknologi yang bersesuaian untuk mengawal aktiviti *video/web conferencing, video streaming, chat, downloading* adalah digalakkan bagi menguruskan penggunaan jalur lebar (*broadband*) yang maksimum dan lebih berkesan; e) Penggunaan Internet hanyalah untuk **kegunaan rasmi sahaja**. Walaubagaimanapun Ketua Jabatan berhak menentukan pengguna yang dibenarkan menggunakan internet atau sebaliknya; f) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh SUB (BPM) / ICTSO / pegawai yang diberi kuasa;	Pentadbir Rangkaian; Pengguna

BIDANG 05 KAWALAN CAPAIAN *(A.9 Access control)*	
g) Penggunaan Internet hanyalah untuk kegunaan rasmi dan berkaitan dengan bidang kerja. Permohonan penggunaan internet bagi tujuan selain kegunaan rasmi hendaklah melalui Ketua Jabatan dan diluluskan oleh Pengurus ICT / ICTSO / Ketua Unit (KnR). h) Bahan yang diperolehi dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; i) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Bahagian/Ketua Seksyen/Pegawai yang diberi kuasa sebelum dimuat naik ke Internet; j) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; k) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh PEJABAT SUK SELANGOR; l) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CDO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; m) Penggunaan *modem/router* untuk tujuan sambungan ke Internet selain daripada yang disediakan oleh BPM tidak dibenarkan sama sekali; dan n) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut;- (i) Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video dan lagu yang boleh menjejaskan tahap capaian Internet; dan (ii) Menyedia, memuat naik, memuat turun dan menyimpan material, teks, ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah dan apa-apa yang boleh mengancam ketenteraman awam.	

BIDANG 05 KAWALAN CAPAIAN *(A.9 Access control)*	
0504 Kawalan Capaian Sistem Pengoperasian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; b) Membekalkan kemudahan kata kunci untuk pengesahan. c) Menghadkan masa penggunaan sistem (time-out) sekiranya tidak aktif dalam masa tertentu. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan; b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf super user; c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem; dan d) Menyediakan tempoh penggunaan mengikut kesesuaian. Perkara-perkara yang perlu dipatuhi termasuk berikut: a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; b) Mewujudkan satu pengenalan diri (*ID*) yang unik dan hanya digunakan oleh pengguna berkenaan sahaja dan satu teknik pengesahan yang bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna; c) Menghadkan dan mengawal penggunaan program utiliti yang berkemampuan bagi satu tempoh yang ditetapkan; d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	Pentadbir Sistem

BIDANG 05 KAWALAN CAPAIAN *(A.9 Access control)*	
0505 Kawalan Capaian Aplikasi dan Maklumat	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdpat di dalam sistem aplikasi.	
050501 Capaian Aplikasi dan Maklumat	
Bertujuan melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di PEJABAT SUK SELANGOR adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut perlu dipatuhi: a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian, keselamatan dan sensitiviti maklumat yang telah ditentukan; b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini; c) Memaparkan notis pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d) Disarankan untuk menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; e) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan f) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah dibolehkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	Pentadbir Sistem; Pengguna
050502 Prosedur *Secure Log-on*	
Capaian kepada sistem dan aplikasi hendaklah dikawal melalui prosedur *Log-on* mengikut keperluan. Bahagian hendaklah mengenal pasti teknik pengesahan *log-on* yang sesuai seperti berikut : a) Tidak memaparkan sistem atau aplikasi selagi proses log-on tidak berjaya. b) Paparkan suatu amaran bahawa sistem atau aplikasi hanya boleh diakses oleh pengguna yang sah. c) Pengesahan log-on. d) Perlindungan terhadap Brute Force log-on adalah disarankan. (contoh: penggunaan captcha atau setaraf) e) Log “aktiviti log on” yang berjaya dan tidak Berjaya. f) Mengadakan amaran keselamatan jika ada potensi percubaan atau pencerobohan log-on berjaya dikesan. g) Memaparkan tarikh dan masa log-on setelah selesai log-on yang Berjaya	Pentadbir Sistem; Pengguna

BIDANG 05 KAWALAN CAPAIAN *(A.9 Access control)*	
h) Tidak memaparkan kata laluan i) Tidak menghantar kata laluan dalam “clear-text” melalui rangkaian j) Menamatkan sesi yang tidak aktif selepas tempoh yang tertentu. k) Menghadkan sesi sambungan sekatan untuk aplikasi yang berisiko tinggi.	Pentadbir Sistem; Pengguna
0506 Peralatan Mudah Alih dan Jarak Jauh	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan jarak jauh.	
050601 Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut:- a) Peralatan mudah alih** hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan. **Laptop, notebook, tablet, dan lain-lain. b) Memastikan peralatan mudah alih yang dibawa keluar dari pejabat perlu disimpan dan dijaga dengan baik bagi mengelakkan daripada kecurian.	Semua kakitangan SUK dan PDT
050602 Kerja Luar Pejabat	
Perkara yang perlu dipatuhi adalah seperti berikut:- a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua kakitangan SUK dan PDT
050603 *Bring Your Own Device (BYOD)*	
Perkara yang perlu dipatuhi adalah seperti berikut:- a) Pengguna BYOD perlu memastikan keselamatan maklumat semasa menggunakan peralatan BYOD; b) Pengguna BYOD adalah dilarang memasang perisian yang tidak dibenarkan oleh PEJABAT SUK SELANGOR; c) Pengguna BYOD adalah dilarang memasang perisian yang mengganggu servis rangkaian PEJABAT SUK SELANGOR; d) Mengaktifkan fungsi keselamatan katalaluan di setiap komputer riba / peranti; e) Perkakasan BYOD hendaklah dilindungi oleh perisian Antivirus bagi mengelak penyebaran virus/malware/trojan dan lain-lain ke atas pengguna PEJABAT SUK SELANGOR yang lain; f) Pengguna BYOD perlu memastikan peranti yang digunakan menggunakan teknologi penyulitan (encryption), tandatangan digital atau sebarang mekanisme bagi melindungi maklumat elektronik semasa ianya digunakan; g) Pengguna BYOD adalah dilarang menyalin dan membawa keluar maklumat organisasi dengan menggunakan peranti mudah alih dan media storan seperti USB, external HD dsb; h) Pengguna BYOD perlu memadam dokumen elektronik dengan merincih secara elektronik/’secure deletion’ selepas dokumen tidak lagi digunapakai; dan i) Pengguna BYOD adalah dilarang meninggalkan komputer riba / peranti di ruang pejabat yang terbuka tanpa menguncikannya dengan kabel keselamatan	Semua kakitangan SUK dan PDT

BIDANG 05 KAWALAN CAPAIAN *(A.9 Access control)*	
0507 Penggunaan Media Sosial	
Objektif: Memahami dan mematuhi asas dalam penggunaan dan pemantauan media sosial dalam sektor awam bagi memastikan penggunaan media sosial dan pengaliran maklumat yang telus, berhemah dan memberi impak positif kepada sektor awam.	
050701 Amalan Baik Pemaparan Media Sosial	
Media sosial merujuk kepada sejenis saluran komunikasi dalam talian yang membolehkan pengguna berinteraksi dengan mudah secara bebas, berkongsi dan membincangkan maklumat dengan menggunakan gabungan multimedia yang terdiri daripada teks, gambar, video dan audio. Pentadbir sistem yang mengendalikan media sosial digalakkan untuk memasukkan kriteria dan kandungan yang relevan dengan PEJABAT SUK SELANGOR seperti yang berikut mengikut kesesuaian kategori jenis media sosial yang digunakan: a) Memaparkan perkataan "<jenis media sosial> Rasmi PEJABAT SUK SELANGOR" b) Meletakkan jata Kerajaan Negeri dan logo rasmi (jika ada) dengan jelas. c) Menyediakan penyataan pengenalan media sosial. d) Menyediakan kandungan dalam bidang kuasa rasmi. e) Memastikan bahasa yang digunakan mudah difahami oleh pengguna.	Pentadbir Sistem
050702 Panduan Umum Penggunaan Media Sosial	
Pentadbir sistem perlu memastikan pelaksanaan panduan umum penggunaan media sosial seperti yang berikut: a) Mengenal pasti objektif utama penggunaan media sosial. b) Memahami cara penggunaan setiap media sosial sebelum menggunakannya. c) Mematuhi Kod Etika Perkhidmatan Awam dalam penggunaan media sosial dan mendapatkan khidmat nasihat sekiranya diperlukan. d) Memastikan akaun media sosial rasmi adalah milik PEJABAT SUK SELANGOR dan bukan milik individu. e) Menggunakan platform media sosial yang mempunyai penggunaan yang tinggi di kalangan kumpulan sasaran atau rakyat. f) Mengikuti perkembangan media sosial terkini bagi memastikan penggunaannya di kalangan rakyat sentiasa berkembang maju. g) Mengelakkan daripada mewujudkan akaun media sosial yang tidak mampu diselaras dandipantau. h) Mengelakkan komunikasi dengan pengguna yang bersikap agresif atau kasar.	Pentadbir Sistem

BIDANG 05 KAWALAN CAPAIAN *(A.9 Access control)*	
050703 Kawalan Keselamatan Penggunaan Media Sosial	
Aspek tanggungjawab pengguna yang berkaitan dengan pengurusan keselamatan media sosial: a) memastikan alamat emel dan kata laluan rasmi tidak digunakan dalam akaun peribadi media sosial. b) mengelakkan sama sekali daripada membenarkan individu lain menggunakan identiti dan kata laluan akaun pegawai awam. c) keluar dari media sosial apabila tidak digunakan bagi mengelakkan kecurian identiti. d) mengelakkan perkongsian maklumat peribadi daripada dimanipulasikan oleh pihak yang tidak bertanggung jawab. e) mengelakkan dari memuat turun aplikasi yang tidak diketahui tahap keselamatannya.	Pentadbir Sistem, Pengguna
050704 Penggunaan Peribadi Media Sosial	
Penggunaan media sosial di kalangan pegawai awam adalah tertakluk kepada peraturan-peraturan yang sedang berkuat kuasa bagi memastikan penggunaan media ini tidak menjejaskan perkhidmatan awam dan pegawai awam tersebut.	Semua kakitangan SUK dan PDT
050705 Etika Penggunaan Media Sosial oleh Pegawai Awam	
Sepanjang menggunakan media sosial samada untuk tujuan rasmi atau peribadi, pegawai awam perlu memastikan etika penggunaan media sosial seperti yang berikut: a) Semua pegawai awam adalah terikat dengan terma dan syarat yang terkandung dalam Peraturan-peraturan Pegawai Awam (Kelakuan dan Tatatertib) 1993 dan arahan-arahan yang berkaitan yang menjadi teras kepada keperibadian atau tatakelakuan anggota perkhidmatan awam. b) Prinsip-prinsip penggunaan media sosial oleh pegawai awam sama ada dalam urusan rasmi ataupun peribadi adalah sama seperti yang terpakai bagi media-media yang lain. c) Pegawai awam tidak digalakkan untuk menggunakan media sosial bagi tujuan peribadi semasa waktu pejabat samada menerusi peralatan komputer atau alat mudah alih yang dibekalkan oleh pejabat ataupun melalui peralatan peribadi. d) Pegawai awam boleh menggunakan media sosial secara peribadi di luar waktu pejabat tetapi perlu berhati-hati supaya tidak mendedahkan sebarang maklumat rasmi. e) Sebarang komen mengenai isu-isu yang melibatkan pentadbiran kerajaan atau yang berbentuk serangan peribadi hendaklah dielakkan. f) Ketepatan dan sensitiviti maklumat yang ingin disampaikan hendaklah disemak terlebih dahulu sebelum dihantar. g) Pegawai awam perlu memastikan perkongsian dan penggunaan maklumat yang berkaitan dengan hak cipta dan harta intelek telah mendapat kebenaran daripada pihak yang berkenaan. h) Sekiranya terdapat kesilapan pada sebarang maklumat yang telah dihebahkan, akui pada umum, buat pembetulan dan mohon maaf kepada pihak yang berkaitan secara terus dalam laman sosial yang terlibat.	Semua

BIDANG 06 KRIPTOGRAFI (A.10 Cryptography)	
0601 Kawalan Kriptografi	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
060101 Enkripsi	
Pengguna hendaklah membuat penyulitan (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi (Sulit dan Terhad Sahaja) pada setiap masa.	Pengguna
060102 Tandatangan Digital – tiada penggunaan buat masa ini	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Pentadbir Sistem; Pengguna
060103 Kawalan Penggunaan Kriptografi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Membangun dan melaksanakan peraturan enkripsi untuk melindungi maklumat sensitif menggunakan kaedah kriptografi yang sesuai pada setiap masa; b) Mengenal pasti tahap perlindungan pengunaan kriptografi dengan mengambil kira jenis, kekuatan dan kualiti algoritma yang diperlukan.	Pentadbir Sistem; Pengguna
060104 Penggunaan Infrastruktur Kunci Awam (PKI)	
Pengurusan ke atas Infrastruktur Kunci Awam (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Pentadbir Sistem

BIDANG 07 KESELAMATAN FIZIKAL DAN PERSEKITARAN (A.11 Physical and environmental security)	
0701 Keselamatan Kawasan	
Objektif: Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
070101 Kawasan Larangan Lokasi ICT	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada warga SUK SELANGOR yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di SUK SELANGOR adalah Pusat Data dan bilik *Server*. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas premis tersebut adalah seperti berikut: a) Sumber data atau server, peralatan komunikasi dan storan perlu ditempatkan di pusat data yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegah kebakaran; b) Akses adalah terhad kepada warga SUK SELANGOR yang telah diberi kuasa sahaja dan dipantau pada setiap masa; c) Pemantauan dibuat menggunakan Sistem CCTV atau peralatan-peralatan lain yang sesuai; d) Peralatan keselamatan seperti CCTV dan pengimbas biometrik perlu diperiksa secara berjadual; e) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; f) Pembekal yang dibawa masuk perlu diiringi oleh pegawai yang bertanggungjawab sehingga ke dalam Pusat Data. Sepanjang pembekal berada dalam Pusat Data, pemantauan adalah melalui CCTV. g) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan dan laluan awam; h) Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; i) Memperkukuhkan dinding dan siling; dan j) Mengehadkan jalan keluar masuk.	Pentadbir Pusat Data
070102 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut:- a) Setiap pengguna PEJABAT SUK SELANGOR hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas;	Semua

BIDANG 07 KESELAMATAN FIZIKAL DAN PERSEKITARAN *(A.11 Physical and environmental security)*	
b) Semua pas keselamatan hendaklah diserahkan balik kepada PEJABAT SUK SELANGOR apabila pengguna berhenti atau bersara; c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama PEJABAT SUK SELANGOR. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan d) Kehilangan pas mestilah dilaporkan dengan segera.	
0702 Keselamatan Peralatan	
Objektif: Melindungi peralatan ICT PEJABAT SUK SELANGOR dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
070201 Peralatan ICT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; c) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; d) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; e) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; g) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salah guna; h) Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan aset ICT di bawah kawalannya; i) Peralatan-peralatan kritikal perlu disokong oleh UPS; j) UPS yang berkuasa tinggi perlu diletakkan di bilik yang berasingan bersuhu rendah yang dilengkapi dengan pengudaraan yang sesuai;	Semua

BIDANG 07
KESELAMATAN FIZIKAL DAN PERSEKITARAN *(A.11 Physical and environmental security)*

k) Semua peralatan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam bilik atau rak berkunci;

l) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;

m) Pegawai Penyelaras Aset (BPM) yang hendak dibawa keluar dari premis PEJABAT SUK SELANGOR, perlulah mendapat kelulusan Pegawai Penyelaras Aset (BPM) atau Pegawai Aset Bahagian dan direkodkan bagi tujuan pemantauan;

n) Pegawai Penyelaras Aset (BPM) yang hilang hendaklah dilaporkan kepada Ketua Jabatan/Bahagian/Seksyen dan Pegawai Penyelaras Aset (BPM) dengan segera;

o) Pegawai Penyelaras Aset (BPM) yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur kehilangan aset dalam Tatacara Pengurusan Aset yang sedang berkuatkuasa.

p) Pengendalian aset ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa;

q) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Penyelaras Aset (BPM);

r) Sebarang kerosakan aset ICT hendaklah dilaporkan kepada Pegawai Penyelaras Aset (BPM) untuk dibaik pulih;

s) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

t) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;

u) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*Administrator Password*) yang telah ditetapkan oleh Pentadbir Sistem ICT;

v) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;

w) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan *"OFF"* apabila meninggalkan pejabat;

x) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan

y) Memastikan plag dicabut daripada suis utama (*Main Switch*) bagi mengelakkan kerosakan perkakasan (selain daripada perkakasan pusat data) sebelum meninggalkan Pejabat terutama pada musim perayaan yang panjang bagi mengelakkan sebarang bencana berlaku.

BIDANG 07 KESELAMATAN FIZIKAL DAN PERSEKITARAN *(A.11 Physical and environmental security)*	
070202 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* dan media-media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Bagi menjamin keselamatan, langkah-langkah berikut perlu diambil: a) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; b) Bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu; c) Semua media storan data yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat; d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan (*data safe*) yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; e) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; f) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; g) Storan dan peralatan *backup* hendaklah disimpan di lokasi yang berasingan yang lebih privasi dan tidak terbuka kepada umum. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; h) Akses dan pergerakan kepada media storan yang mempunyai data kritikal perlu direkodkan; i) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; dan j) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	Semua

BIDANG 07 KESELAMATAN FIZIKAL DAN PERSEKITARAN *(A.11 Physical and environmental security)*	
070203 Media Tandatangan Digital – tiada penggunaan buat masa ini	
Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah–langkah berikut: Pengguna hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; a) Tidak boleh dipindah-milik atau dipinjamkan; dan b) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan selanjutnya mengikut Prosedur Pelaporan Insiden.	Semua
070204 Media Perisian Dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perisian-perisian ICT yang disokong oleh BPM untuk pemasangan, penyelenggaraan dan latihan adalah termasuk: i. MS Office yang terdiri daripada: • MS Word • MS Excel • MS Powerpoint • MS Outlook / Outlook Web Access (OWA) ii. Web Browser iii. Acrobat Reader iv. WinZip / File Compress v. Antivirus vi. Dewan Eja vii. Sistem Kewangan Kerajaan viii. Software Cleaning b) Sokongan untuk perisian yang tidak tersenarai di item (a) seperti perisian Open Office hanya akan diberikan sekiranya ada tenaga kepakaran di BPM; c) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan PEJABAT SUK SELANGOR. Pengguna dilarang memasang (install) perisian ICT yang tidak berdaftar, berlesen, cetak rompak atau perisian yang dibeli sendiri pada mana-mana aset ICT PEJABAT SUK SELANGOR; d) Pihak BPM boleh mengesan dan berhak membuang (uninstall) perisian yang tidak diperakui tanpa perlu mendapat kebenaran pengguna; e) Pengguna tidak dibenarkan membuang sebarang perisian yang telah dipasang oleh BPM di dalam PC atau komputer riba masing-masing; f) Pengguna mesti memastikan media storan (disket, CD/DVD, External Hard Drive atau thumb drive) yang menyimpan dokumen terperingkat disimpan di tempat yang selamat; dan g) Pengguna mesti memastikan maklumat rahsia rasmi yang terkandung dalam media storan seperti pita magnetik, cakera keras, CD/DVD, *optical disk, removal disk (thumb/PenDrive/ External Hard Drive)* dan lain-lain, dikawal dan dilindungi dengan perisian penyulitan (encryption) yang disyorkan oleh BPM.	Pentadbir Sistem

BIDANG 07
KESELAMATAN FIZIKAL DAN PERSEKITARAN *(A.11 Physical and environmental security)*

070205 Pelupusan

Pelupusan melibatkan semua aset ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau aset bernilai rendah yang dibekalkan oleh PEJABAT SUK SELANGOR dan ditempatkan di PEJABAT SUK SELANGOR dan Pejabat-pejabat Daerah Negeri Selangor. Langkah-langkah berikut perlu diambil dalam memastikan aset ICT dilupuskan dengan teratur: a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding*, *grinding*, *degaussing* atau pembakaran; b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; c) Pegawai Penyelaras Aset (BPM) akan mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; d) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; e) Pegawai Penyelaras Aset (BPM) bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem e-Aset; f) Pelupusan peralatan ICT boleh dilakukan secara berpusat/tidak berpusat mengikut tatacara pelupusan semasa yang berkuat kuasa; g) Peralatan-peralatan ICT yang akan dilupuskan hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; h) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:- i) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya; ii) Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian PEJABAT SUK SELANGOR; dan iii) Memindah keluar dari PEJABAT SUK SELANGOR mana- mana peralatan ICT yang hendak dilupuskan; i) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan. j) Pelupusan aset ICT adalah tertakluk kepada 1 Pekeliling Perbendaharaan (1PP) Pengurusan Aset bertajuk “Tatacara Pengurusan Aset Alih Kerajaan” atau pekeliling terbaharu yang berkuatkuasa.	Pegawai Penyelaras Aset (BPM); Pengguna

BIDANG 07 KESELAMATAN FIZIKAL DAN PERSEKITARAN *(A.11 Physical and environmental security)*	
070206 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut: a) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; b) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f) Bantuan teknikal/ aduan tentang masalah-masalah yang dihadapi dalam penggunaan ICT hendaklah dilaporkan melalui Sistem E-helpdesk (https://ehelpdesk.selangor.gov.my) atau Helpdesk Bahagian Pengurusan Maklumat (BPM) – 03-55447569.	Semua
070207 Peralatan ICT yang dibawa keluar premis	
Peralatan ICT yang dibawa keluar dari premis PEJABAT SUK SELANGOR adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Peralatan perlu dilindungi dan dikawal sepanjang masa; b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan sebarang kehilangan peralatan adalah di bawah tanggungjawab individu yang membawa keluar peralatan tersebut.	Semua
0703 Keselamatan Persekitaran	
Objektif: Melindungi aset ICT PEJABAT SUK SELANGOR dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
070301 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk perolehan, menyewa, mengubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada SUB (BPM) dan SUB (BKP) mengikut yang berkenaan.	Semua

BIDANG 07 KESELAMATAN FIZIKAL DAN PERSEKITARAN *(A.11 Physical and environmental security)*	
Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b) Semua ruang pejabat khususnya yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; g) Semua peralatan perlindungan hendaklah disemak dan diuji. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan h) Akses kepada saluran *riser dan* rak *switches* hendaklah sentiasa dikunci.	
070302 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan bekalan kuasa: a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b) Peralatan sokongan seperti UPS dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik *server* supaya mendapat bekalan kuasa berterusan; dan c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	(BKP); Pentadbir Pusat Data
070303 Kabel	
Kabel komputer/rangkaian hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:-	Pentadbir Rangkaian

BIDANG 07 KESELAMATAN FIZIKAL DAN PERSEKITARAN *(A.11 Physical and environmental security)*	
a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	
070304 Prosedur Kecemasan -	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan PEJABAT SUK SELANGOR; dengan merujuk kepada Garis Panduan MAMPU 2011; dan b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut Jabatan.	Semua
0704 Keselamatan Dokumen	
Objektif: Melindungi maklumat PEJABAT SUK SELANGOR dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan sistem dokumentasi: a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada; c) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; d) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; e) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; f) Pelupusan dokumen hendaklah mengikut Prosedur Keselamatan semasa seperti mana Arahan Keselamatan (Semakan dan pindaan 2017), Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan g) Menggunakan penyulitan *(encryption)* ke atas dokumen rahsia rasmi yang disediakan bertaraf sulit dan terhad sahaja boleh disimpan dan dihantar secara elektronik.	Semua

BIDANG 07 KESELAMATAN FIZIKAL DAN PERSEKITARAN *(A.11 Physical and environmental security)*	
0705 Kawalan Peralatan yang ditempatkan secara sementara/ Peralatan Sewaan / Peralatan Ujicuba *(Proof of Concept)*	
Objektif: Melindungi peralatan PEJABAT SUK SELANGOR dari sebarang bentuk ancaman	
a) Penerimaan i. peralatan yang diterima bebas daripada virus, pencerobohan *backdoor*, *worm* dan perkara-perkara yang boleh memberi ancaman kepada perkhidmatan ICT jabatan. b) Penyelenggaraan i. capaian melalui rangkaian luar PEJABAT SUK SELANGOR adalah tidak dibenarkan; dan ii. aktiviti penyelenggaraan adalah di bawah pengawasan pegawai PEJABAT SUK SELANGOR. c) Pemulangan i. maklumat yang tersimpan dalam storan perlu dihapuskan secara kekal (secured delete); dan ii. memastikan semua maklumat Jabatan tidak tertinggal pada peralatan.	Semua

BIDANG 08 PENGURUSAN OPERASI (A.12 Operational security)	
0801 Pengurusan Prosedur Operasi	
Objektif: Memastikan pengurusan operasi dan kemudahan pemprosesan maklumat berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.	
080101 Pengendalian Dokumen Prosedur Operasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua
080102 Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Pengubahsuaian melibatkan perkakasan, sistem pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran SUB (BPM), pegawai atasan atau pemilik aset ICT terlebih dahulu; b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskinikan mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau sebaliknya; dan e) Setiap perubahan hendaklah direkodkan	Semua
080103 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset	Pentadbir Sistem

BIDANG 08 PENGURUSAN OPERASI *(A.12 Operational security)*	
ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. d) Pemilik sistem hendaklah bertanggungjawab sepenuhnya ke atas pengurusan pengasingan tugas dan tanggungjawab kakitangan dan pembekal.	
0802 Perancangan dan Penerimaan Sistem	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
080201 Perancangan Kapasiti	
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem; Pentadbir Rangkaian;
080202 Penerimaan Sistem	
Perkara -perkara yang perlu dipatuhi adalah seperti berikut: a) Semua sistem baru termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. b) Sebarang penyerahan atau penerimaan sistem baru perlu mendapat pengesahan/kelulusan pemilik sistem dan perlu melalui proses UAT (*User Acceptance Test)* dan FAT *(Final Acceptance Test);* dan c) Penyelenggaraan sistem tersebut adalah berdasarkan manual operasi dan prosedur yang ditetapkan. Semua sistem baharu (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. Kriteria ini hendaklah merangkumi perkara berikut:- a) Memenuhi kehendak dan keperluan pengguna; b) Menggunakan perisian pembangunan yang sah; c) Memenuhi ciri-ciri keselamatan bagi mengelakkan risiko pencerobohan dan sebagainya; dan d) Memenuhi keperluan-keperluan teknologi semasa dan akan datang (Contoh: mampu menggunakan pelbagai platform, IPv6 *ready*).	Pentadbir Sistem; Pengguna

BIDANG 08 PENGURUSAN OPERASI *(A.12 Operational security)*	
0803 Perisian Berbahaya	
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya.	
080301 Perlindungan dari Perisian Berbahaya	
Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT dari perisian berbahaya: a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, dan IPS mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa; c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; d) Mengemas kini paten antivirus dengan yang terkini; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	Pentadbir Sistem; Pengguna
080302 Perlindungan dari *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Pentadbir Sistem
0804 Housekeeping	
Objektif: Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
080401 Backup	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. *Backup* hendaklah direkodkan dan disimpan di *off site*, di antaranya adalah:	

BIDANG 08 PENGURUSAN OPERASI *(A.12 Operational Security)*	
a) Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaharu; b) Membuat backup ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan backup bergantung pada tahap kritikal maklumat; c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d) *Backup* hendaklah dilaksanakan secara harian, mingguan, bulanan dan/atau tahunan. Kekerapan *backup* bergantung pada tahap kritikal maklumat; e) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	
0805 Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
080501 Pengauditan dan Forensik ICT	
ICTSO mestilah bertanggungjawab merekod dan menganalisa perkara-perkara berikut:- a) Sebarang percubaan pencerobohan kepada sistem ICT PEJABAT SUK SELANGOR; b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery*, *phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f) Aktiviti instalasi dan penggunaan perisian yang membebankan *bandwith* rangkaian; g) Aktiviti penyalahgunaan akaun e-mel; h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran pentadbir rangkaian BPM; dan	ICTSO

BIDANG 08 PENGURUSAN OPERASI *(A.12 Operational security)*	
i) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian.	
080502 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut:- a) Rekod setiap aktiviti transaksi; b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan d) Maklumat akitiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Pentadbir Sistem yang berkaitan hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Sistem
080503 Sistem Log	
Fungsi-fungsi sistem log adalah seperti berikut: a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c) Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	Pentadbir Sistem
080504 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;	Pentadbir Sistem

BIDANG 08 PENGURUSAN OPERASI *(A.12 Operational security)*	
d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisa dan diambil tindakan sewajarnya; dan f) Masa yang berkaitan dengan sistem pemprosesan maklumat dalam PEJABAT SUK SELANGOR atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.	
0806 Kawalan Teknikal Keterdedahan (*vulnerability*)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
080601 Kawalan dari Ancaman Teknikal	
Maklumat mengenai ancaman teknikal sistem maklumat yang digunakan perlu diperolehi. Pendedahan organisasi kepada ancaman teknikal perlu dinilai bagi mengenalpasti tahap risiko yang bakal dihadapi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem
080602 Pematuhan Keperluan Audit	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua

BIDANG 09
PENGURUSAN KOMUNIKASI (A.13 Communications security)

0901 Pengurusan Keselamatan Rangkaian

Objektif :
Memastikan perlindungan pemprosesan maklumat di dalam rangkaian.

090101 Kawalan Infrastruktur Rangkaian

Infrastruktur Rangkaian perlu dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Langkah-langkah bagi menangani ancaman ke atas rangkaian adalah seperti berikut: a) Sebarang penambahan dan pengujian peralatan atau perisian rangkaian baharu kepada rangkaian PEJABAT SUK SELANGOR, perlu membuat permohonan kepada BPM terlebih dahulu. b) Segmen operasi dan rangkaian hendaklah diasingkan dengan segmen komputer pengguna untuk mengawal capaian dan pengubahsuaian yang tidak dibenarkan; c) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; d) Semua peralatan mestilah melalui proses UAT semasa pemasangan dan konfigurasi; e) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; f) Semua capaian kepada Internet dan sistem aplikasi mestilah melalui *firewall* dan dikawal oleh BPM; g) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan PEJABAT SUK SELANGOR; h) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran BPM; i) Memasang perisian IPS bagi mengesan dan menghalang sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat PEJABAT SUK SELANGOR, j) Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; k) Semua pengguna hanya dibenarkan menggunakan rangkaian yang disediakan oleh PEJABAT SUK SELANGOR. Penggunaan *modem* adalah dilarang sama sekali; l) Sebarang penyambungan ke rangkaian luar yang bukan di bawah kawalan PEJABAT SUK SELANGOR adalah tidak dibenarkan, kecuali mendapat kebenaran BPM; m) Kemudahan bagi *Wireless* LAN perlu dipastikan kawalan keselamatan (kata laluan); dan	Pentadbir Rangkaian

BIDANG 09 PENGURUSAN KOMUNIKASI *(A.13 Communications security)*	
n) Semua capaian dari luar rangkaian PEJABAT SUK SELANGOR kepada sistem dalaman yang tidak boleh diakses dari luar, mestilah menggunakan *Virtual Private Network* (VPN) dan dikawal oleh BPM (PDRK);	
090102 Keselamatan Perkhidmatan Rangkaian	
Pengurusan bagi semua perkhidmatan rangkaian yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenalpasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian.	Pentadbir Rangkaian;
090103 Pengasingan Rangkaian	
Pengasingan rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian Pejabat SUK Selangor.	Pentadbir Rangkaian;
0902 Pengurusan Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
090201 Penghantaran dan Pemindahan Media Mudah Alih	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada SUB (BPM) / pemilik sistem terlebih dahulu.	Semua
090202 Prosedur Pengendalian Media	
Di antara prosedur-prosedur pengendalian media yang perlu dipatuhi termasuk: a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e) Menyimpan semua media di tempat yang selamat; dan f) Media yang mengandungi maklumat terperingkat hendaklah dihapus atau dimusnahkan mengikut peraturan dan prosedur yang betul dan selamat.	Pentadbir Sistem; Pengguna
090203 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	Semua

BIDANG 09 PENGURUSAN KOMUNIKASI *(A.13 Communications security)*	
0903 Pengurusan Pertukaran Maklumat	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara PEJABAT SUK SELANGOR/agensi dan mana-mana entiti luar terjamin.	
090301 Pertukaran Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara PEJABAT SUK SELANGOR dengan pihak luar; c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari PEJABAT SUK SELANGOR; dan d) Maklumat yang terdapat dalam e-mel perlu dilindungi sebaik-baiknya;	Pentadbir Sistem; Pengguna
090302 Pengurusan Mel Elektronik (E-mel)	
Penggunaan e-mel di PEJABAT SUK SELANGOR hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Tatacara Penggunaan Bagi Capaian Internet, Intranet, E-Mel dan Broadband Tanpa Wayar Bagi Tujuan Pengurusan dan Pentadbiran”; “Garis Panduan Penggunaan Mel Elektronik Pejabat SUK Selangor” dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara – perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: a) Akaun e-mel rasmi bukanlah hak mutlak seseorang. Ia adalah kemudahan yang tertakluk kepada peraturan jabatan dan boleh ditarik balik jika penggunaannya melanggar peraturan; b) Pengguna adalah bertanggungjawab kepada akaun e-mel masing-masing. PEJABAT SUK SELANGOR tidak akan bertanggungjawab ke atas sebarang kesalahan jenayah dan seumpamanya berkaitan e-mel; c) Menyebar perisian cetak rompak atau maklumat berbau politik, hasutan atau perkauman atau apa-apa maklumat yang menjejaskan reputasi PEJABAT SUK SELANGOR dan perkhidmatan awam melalui kemudahan e-mel Selangor adalah dilarang; d) Akaun atau alamat e-mel yang diperuntukkan oleh PEJABAT SUK SELANGOR sahaja boleh digunakan. Penggunaan akaun milik orang lain adalah dilarang; e) Permohonan E-mel hendaklah dibuat dengan melengkapkan Borang “Borang Pengurusan E-mel dan Internet” yang boleh diperolehi dari Portal Selangor atau Bahagian Teknologi Maklumat, SUK SELANGOR;	Pentadbir E-mel; Pengguna

BIDANG 09 PENGURUSAN KOMUNIKASI *(A.13 Communications security)*	
f) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; g) Had saiz kotak e-mel (*mailbox*) setiap pengguna adalah minimum 2GB dan maksimum 100GB. Had ini ditentukan oleh Pentadbir E-mel mengikut gred atau deskripsi tugas. h) Had penghantaran e-mel termasuk bahan kepilan yang dibenarkan adalah tidak melebihi 30 MB. Pengguna adalah disarankan untuk menggunakan: • kaedah inovatif dalam penghantaran fail bersaiz besar seperti menggunakan kaedah muat turun fail dengan memaklumkan lokasi pautan *Uniform Resource Locator* (URL); • kaedah pemampatan untuk mengurangkan saiz fail dengan memastikan ciri-ciri keselamatan dilaksanakan; • kaedah enkripsi bagi dokumen terperingkat yang dihantar secara elektronik. i) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; j) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; k) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi hendaklah dihapuskan; l) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; m) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; n) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; o) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing; p) Pengguna juga hendaklah memastikan fail yang akan dihantar atau yang diterima melalui kepilan (*attachment*) bebas dari virus dengan melakukan *scanning* dengan perisian antivirus; q) Penghantaran dokumen rasmi hendaklah menggunakan e-mel rasmi jabatan sahaja dan pastikan alamat e-mel penerima adalah betul; r) Penggunaan e-mel PEJABAT SUK SELANGOR bagi tujuan peribadi adalah tidak dibenarkan; s) Pengguna adalah bertanggungjawab untuk mengurus dan memastikan saiz e-mel yang disimpan di dalam peti mail (*mailbox*) masing-masing tidak melebihi kuota saiz *mailbox*. t) Penghantaran lampiran dalam format atau *extension* " *.exe, *.bat " dan " *.com" tidak dibenarkan dan pengguna yang menerima fail berkenaan juga adalah dilarang untuk membuka e-mel tersebut kerana boleh mengakibatkan penyebaran virus;	

BIDANG 09 PENGURUSAN KOMUNIKASI *(A.13 Communications security)*	
u) Hanya kakitangan PEJABAT SUK SELANGOR atau pengguna yang dibenarkan sahaja boleh dipertimbangkan untuk mendapat kemudahan e-mel rasmi jabatan; v) Fungsi *Auto-Reply* adalah tidak dibenarkan kecuali pengguna yang bercuti atau bertugas di luar pejabat iaitu dengan menggunakan mesej *Out-of-Office*; w) Pengguna adalah dilarang sama sekali menggunakan alamat e-mel rasmi Selangor bagi pendaftaran dalam mana-mana web/kumpulan/forum yang tidak berkaitan dengan urusan kerja rasmi; dan x) Bahagian Sumber Manusia PEJABAT SUK SELANGOR perlu memaklumkan sebarang status pengguna (bertukar jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke PEJABAT SUK SELANGOR) di bahagian masing-masing bagi tujuan pengemaskinian e-mel yang terlibat; y) Akaun e-mel pengguna yang tidak aktif melebihi antara 30 hingga 90 hari akan dibekukan penggunaannya dan seterusnya dihapuskan selepas 30 hari kecuali dimaklumkan kepada Pentadbir E-mel. z) Capaian e-mel kakitangan PEJABAT SUK SELANGOR yang tidak lagi berkhidmat di PEJABAT SUK SELANGOR akan dihentikan serta-merta kecuali dimaklumkan kepada Pentadbir E-mel. Perlanggaran kepada mana-mana peraturan boleh menyebabkan penggantungan akaun pengguna atau mana-mana tindakan tatatertib yang bersesuaian.	
0904 Perkhidmatan E-Dagang (*Electronic Commerce Services*)	
Objektif : Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.	
090401 E-Dagang	
Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan internet. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b) Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Pentadbir Sistem; Pengguna

BIDANG 09 PENGURUSAN KOMUNIKASI *(A.13 Communications security)*	
090402 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut:- a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Semua

BIDANG 10
PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM *(A.14 System acquisition, development and maintenance)*

1001 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif:
Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

100101 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketetapan maklumat; b) Pengujian aplikasi hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan sistem *output* untuk memastikan data yang telah diproses adalah tepat; c) Aplikasi perlu melalui proses pengesahan data (*data validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	SUB (BPM); ICTSO; Pemilik Sistem; Pentadbir Sistem

100102 Pengesahan Data *Input* dan *output*

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b) Data *Output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pentadbir Sistem

100103 Kawalan Prosesan

Kawalan proses perlu ada dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan terhasil daripada masalah semasa prosesan.	Pentadbir Sistem

100104 Keselamatan Fail Sistem

Fail sistem perlu dikawal dan dikendalikan dengan baik dan selamat.

a) proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem atau pegawai yang berkenaan;
b) kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji;
c) mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian;
d) mengaktifkan log audit bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; dan
e) data ujian hendaklah dipilih dan penggunaannya dikawal serta dilindungi.

BIDANG 10 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM *(A.14 System acquisition, development and maintenance)*	
100105 Keselamatan Perkhidmatan Aplikasi di Rangkaian Umum	
Maklumat aplikasi yang melalui rangkaian umum (public networks) hendaklah dilindungi daripada aktiviti penipuan dan pendedahan maklumat yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti berikut: a) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (authentication). b) Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi. c) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan perkhidmatan ICT. d) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	ICTSO; Pentadbir Rangkaian; Pentadbir Sistem; Pihak Ketiga
100106 Melindungi Perkhidmatan Transaksi Aplikasi	
Maklumat yang terlibat dalam perkhidmatan transaksi hendaklah dilindungi daripada penghantaran yang tidak lengkap, *misroute*, pengubahan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan dan duplikasi mesej. Perkara yang perlu dipertimbangkan adalah seperti berikut: *(A.14.1.3 Protecting application services transactions)* a) Memastikan semua aspek transaksi dipatuhi: i) Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan ii) Mengekalkan kerahsiaan maklumat iii) mengekalkan privasi pihak yang terlibat iv) Komunikasi antara semua pihak yang terlibat dirahsiakan v) Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi	Pentadbir Rangkaian; Pentadbir Sistem

BIDANG 10 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM *(A.14 System acquisition, development and maintenance)*	
100107 Dasar Keselamatan Dalam Pembangunan Sistem	
Peraturan untuk pembangunan sistem hendaklah diwujudkan dan digunakan untuk perkembangan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti berikut: *(A.14.2.1 Secure development policy)* a) Keselamatan persekitaran pembangunan b) Panduan keselamatan dalam kitar hayat pembangunan (development lifecycle) perisian c) Keselamatan dalam fasa reka bentuk d) Pemeriksaan keselamatan dalam perkembangan projek e) Keselamatan repositori f) Keselamatan dalam kawalan versi g) Keperluan pengetahuan keselamatan dalam pembangunan perisian h) Kebolehan pembekal untuk mengenalpasti kelemahan; dan i) Mencadangkan penambahbaikan dalam pembangunan sistem	Pentadbir Sistem; ICTSO
1002 Keselamatan Dalam Proses Pembangunan dan Sokongan Sistem	
Objektif : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
100201 Prosedur Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkod dan disahkan sebelum diguna pakai; b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal; c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d) Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e) Menghalang sebarang peluang untuk membocorkan maklumat.	Pentadbir Sistem

BIDANG 10 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM *(A.14 System acquisition, development and maintenance)*	
100202 Pembangunan Perisian Secara *Outsource*	
Pembangunan perisian aplikasi secara *outsource* perlu dipantau oleh pemilik sistem. *Source code* adalah menjadi hak milik PEJABAT SUK SELANGOR.	Pentadbir Sistem
1003 Keselamatan Dalam Proses Pembangunan dan Sokongan Sistem	
Objektif : Memastikan keselamatan data yang digunakan	
100301 Perlindungan Data Ujian	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Data dan aturcara yang hendak diuji perlu dipilih, dilindungi dan dikawal. b) Pengujian hendaklah dibuat ke atas aturcara yang terkini. c) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan. *(A.14.3.1 Protection of test data)*	Pemilik Sistem; Pentadbir Sistem

BIDANG 11
HUBUNGAN DENGAN PEMBEKAL/PIHAK KETIGA *(A.15 Supplier relationships)*

1101 Pihak Ketiga

Objektif :
Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain)

110101 Keperluan Keselamatan Kontrak dengan Pihak Ketiga

Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi: a) Membaca, memahami dan mematuhi DKICT PEJABAT SUK SELANGOR; b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d) Akses kepada aset ICT PEJABAT SUK SELANGOR perlu berlandaskan kepada perjanjian kontrak; e) Mengenal pasti risiko ke atas keselamatan maklumat dan memastikan pelaksanaan kawalan yang sesuai ke atas maklumat tersebut; f) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga, dan g) Akses kepada aset ICT PEJABAT SUK SELANGOR perlu berlandaskan perjanjian kontrak. Perjanjian yang dimeterai perlu mematuhi perkara-perkara berikut: a. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga, perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i) *Non-Disclosure Agreement*; ii) Perakuan Akta Rahsia Rasmi 1972; dan h) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT PEJABAT SUK SELANGOR sebagaimana **Lampiran 1**.	Semua kakitangan SUK dan PDT

BIDANG 11
HUBUNGAN DENGAN PEMBEKAL/PIHAK KETIGA *(A.15 Supplier relationships)*

1102 Pengurusan Penyampaian Perkhidmatan Pembekal, Pakar Runding dan Pihak-Pihak Lain Yang Terlibat

Objektif:
Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pembekal, pakar runding dan pihak-pihak lain yang terlibat.

110201 Kawalan Keselamatan Maklumat Melalui Perjanjian Dengan Pembekal

Jabatan/Agensi hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal/pihak ketiga. Perkara yang perlu dipatuhi adalah: a) Memasukkan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat; b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa dan; c) Pengurusan ke atas perubahan penyediaan perkhidmatan termasuk menyelenggara dan menambah baik polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua kakitangan SUK dan PDT

110202 Pengurusan Perubahan Perkhidmatan Pembekal

Perkara yang perlu diambil kira adalah: a) Perubahan dalam perjanjian dengan pembekal; b) Perubahan yang dilakukan oleh Pejabat SUK Selangor bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran kakitangan pembekal dan perubahan sub-kontraktor pembekal.	Semua

BIDANG 12
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN *(A.16 Information security incident management)*

1201 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif :
Untuk memastikan semua insiden dikendalikan dengan cepat, tepat dan berkesan dan memastikan sistem ICT PEJABAT SUK SELANGOR dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej PEJABAT SUK SELANGOR dan sistem penyampaian perkhidmatan.

120101 Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar DKICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan CSIRT SELANGOR dengan kadar segera dan semua maklumat adalah dianggap SULIT: a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e) Berlaku percubaan menceroboh, penyelewengan dan insiden- insiden yang tidak dijangka. Prosedur pelaporan insiden keselamatan ICT berdasarkan: a) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendlian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam c) Surat Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan Pengendalian Insiden Keselamatan Siber Sektor Awam i) **Pelaporan** Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada ICTSO dan kepada Jawatankuasa CSIRT SELANGOR untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat adalah **SULIT,** dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan. ii) **Tanggungjawab Jawatankuasa CSIRT SELANGOR** Jawatankuasa CSIRT SELANGOR akan bertindak menghubungi dan melaporkan insiden yang berlaku kepada NACSA sama ada sebagai input atau untuk tindakan seterusnya.	ICTSO; CSIRT SELANGOR; Pengguna

BIDANG 12 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN *(A.16 Information security incident management)*	
iii) **Tanggungjawab Pengguna** Semua kakitangan, pembekal, pakar runding dan pihak-pihak lain yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan secara sendiri, tapi sebaliknya perlu terus melaporkan dengan segera sebarang kejadian insiden keselamatan ICT, kerentanan yang diperhatikan atau disyaki terdapat dalam sistem maklumat menerusi mekanisme pelaporan ini. Ini adalah bagi mengelakkan kerosakan atau kehilangan bahan bukti pencerobohan dan cubaan menceroboh. iv) **Tanggungjawab Pentadbir Sistem** Pentadbir sistem yang terlibat perlu melaporkan sebarang kejadian yang melibatkan keselamatan ICT kepada CSIRT SELANGOR dan ICTSO (BPM). v) **Tindakan Dalam Keadaan Berisiko Tinggi** Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak.	
1202 Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat Insiden Keselamatan ICT.	
120201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
CSIRT SELANGOR menerima aduan atau laporan daripada pengguna, laporan yang dikesan dari pihak NACSA atau laporan dari sumber lain. Seterusnya, maklumat tentang insiden akan didaftarkan. Siasatan awal atau kajian perlu dijalankan bagi mengenal pasti jenis insiden tersebut. Laporan insiden kemudiannya dimaklumkan kepada pihak NACSA. Sekiranya insiden tersebut memerlukan tindakan undang-undang susulan, laporan dipanjangkan kepada agensi penguatkuasa undang-undang. CSIRT SELANGOR yang diketuai oleh ICTSO akan menjalankan tindakan pengendalian secara capaian jauh (remote) atau on-site. Sekiranya laporan tersebut memerlukan bantuan pihak NACSA, permohonan akan dihantar bagi mendapatkan maklum balas pihak NACSA. Bagi laporan yang memerlukan bantuan daripada CERT agensi yang lain, permohonan akan dihantar melalui pihak NACSA dan khidmat nasihat akan disalurkan. CSIRT SELANGOR seterusnya akan menyediakan laporan dan ICTSO mengesahkan sekiranya PKP perlu diaktifkan atau sebaliknya. Pengesahan akan dihantar kepada CDO bagi mengaktifkan PKP.	ICTSO, CSIRT SELANGOR

BIDANG 12 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN *(A.16 Information security incident management)*	
Laporan insiden yang tidak memerlukan PKP akan diteruskan dengan melaksanakan tindakan bagi tujuan pemulihan. Carta lengkap mengenai perjalanan laporan insiden seperti di **LAMPIRAN 2**.	

BIDANG 13
ASPEK KESELAMATAN MAKLUMAT & PENGURUSAN KESINAMBUNGAN PERKHIDMATAN *(A.17 Information security aspects of business continuity management)*

1301 Dasar Kesinambungan Perkhidmatan

Objektif :
Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

130101 Pelan Pengurusan Kesinambungan Perkhidmatan

Pelan Kesinambungan Perkhidmatan atau PKP (*Business Continuity Plan* – BCP) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh pengurusan tertinggi Kerajaan Negeri Selangor dan perkara-perkara berikut perlu diberi perhatian: a) Mengenal pasti berdasarkan BCP Pejabat alternatif dan/atau b) Mengenal pasti perkhidmatan utama (*core business*) dan proses- proses kritikal di agensi; c) Melaksanakan penilaian risiko dengan mengenal pasti ancaman dan risiko yang boleh mengakibatkan gangguan terhadap perkhidmatan serta impak gangguan tersebut terhadap fungsi kritikal agensi; d) Menentukan strategi bagi memastikan perkhidmatan agensi tetap dapat diteruskan walaupun berlaku gangguan/bencana; e) Mendokumentasikan PKP dan memastikan rekod dan semua dokumentasi diurus dengan baik dan sistematik; f) Melaksanakan simulasi pelan sekurang-kurangnya setahun sekali mengikut kepada prosedur PKP;	CDO; SUB (BKP) SUB (BPM)

130102 Pelan Pengurusan Pemulihan Bencana (*Disaster Recovery Plan*)

Pelan Pemulihan Bencana atau PPB (*Disaster Recovery Plan* – DRP) direka bentuk untuk membantu agensi mengembalikan semula proses perkhidmatan dalam tempoh ditetapkan untuk pemulihan bencana. Ia merujuk kepada dokumen pelan yang menetapkan sumber, 85ejabat85, tanggungjawab dan data yang diperlukan untuk mengurus proses pemulihan selepas berlaku gangguan dalam perkhidmatan agensi. Pelan ini mestilah diluluskan oleh pengurusan atasan BPM dan perkara-perkara berikut perlu diberi perhatian: a) Mengenal pasti pejabat alternatif dan/atau pusat pemulihan bencana (*Disaster Recovery Centre – DRC*) yang berbeza dari lokasi asal bagi meneruskan perkhidmatan apabila lokasi asal menghadapi gangguan/bencana; b) Mengenalpasti peranan dan tanggungjawab Pasukan Pemulihan Bencana serta pembekal berkaitan; c) Mengenalpasti sistem/aplikasi yang memerlukan *backup*;	SUB (BPM); Pasukan Pemulihan Bencana

BIDANG 13 ASPEK KESELAMATAN MAKLUMAT & PENGURUSAN KESINAMBUNGAN PERKHIDMATAN *(A.17 Information security aspects of business continuity management)*	
d) Menyediakan infrastruktur bagi memastikan pemulihan boleh dilaksanakan; e) Mendokumentasikan proses dan prosedur yang digunapakai untuk pemulihan maklumat dan kemudahan yang berkaitan; f) Melaksanakan pengujian dan latihan kepada kakitangan apabila perlu; g) Mengemaskini pelan apabila perlu. PEJABAT SUK SELANGOR hendaklah memastikan salinan Pelan Pemulihan Bencana sentiasa dikemaskini dan dilindungi seperti di lokasi utama.	
1302 Redundancy	
130201 Ketersediaan Kemudahan Pemprosesan Maklumat	
Kemudahan pemprosesan maklumat perlu mempunyai *redundancy* yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan redundancy perlu diuji (failover test) keberkesanannya dari masa ke semasa.	ICTSO; BPM SUK Selangor

BIDANG 14 PEMATUHAN (A.18 *Compliance*)	
1401 Pematuhan dan Keperluan Perundangan	
Objektif Meningkatkan tahap keselamatan ICT bagi mengelak daripada perlanggaran kepada DKICT PEJABAT SUK SELANGOR.	
140101 Pematuhan Dasar	
Setiap pengguna di PEJABAT SUK SELANGOR hendaklah membaca, memahami dan mematuhi DKICT PEJABAT SUK SELANGOR dan undang-undang atau peraturan-peraturan lain yang berkaitan. Semua aset ICT di PEJABAT SUK SELANGOR termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	Semua kakitangan SUK dan PDT, Semua pembekal yang berurusan dengan SUK dan PDT
140102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	
ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO
140103 Keperluan Perundangan	
Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di PEJABAT SUK SELANGOR adalah seperti di **Lampiran 3.**	Pengguna
140104 Pelanggaran Perundangan	
Tindakan undang-undang dan tatatertib boleh diambil ke atas sesiapa yang terlibat di dalam semua perbuatan kecuaian, kelalaian dan perlanggaran keselamatan yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972 dan akta lain yang berkaitan. SUB (BPM) atau ICTSO adalah berhak untuk mengambil tindakan sebagaimana berikut:- i) Membuat teguran pertama melalui e-mel, sistem pemantauan atau mana-mana medium komunikasi secara atas talian; ii) Memberi e-mel/surat teguran kepada pelaku dan satu 87indaka emel akan turut diberi kepada Ketua Jabatan/pegawai pelaku; iii) Pelaku hendaklah memberi surat tunjuk sebab dalam tempoh tiga (3) hari bekerja dari 87indak e-mel/surat diterima; dan iv) Mengambil 87indakan berupa menarik balik kemudahan capaian internet/ peralatan ICT/ 87indakan (sementara/kekal) bergantung kepada jenis dan tahap kesalahan.	Pengguna

Lampiran 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT PEJABAT SUK SELANGOR

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian/Syarikat : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT PEJABAT SUK SELANGOR; dan

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : .....

Tarikh : .....

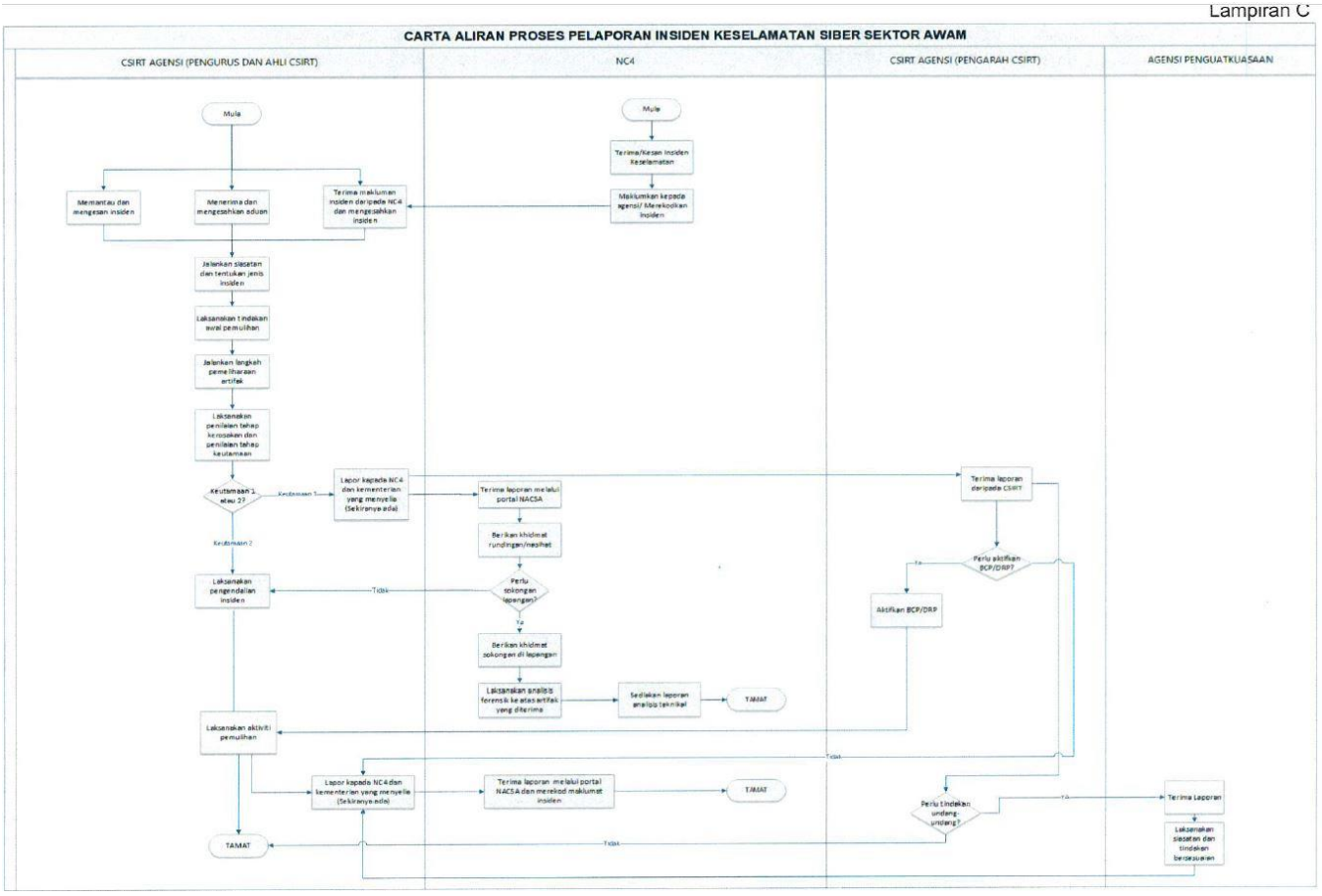
Pengesahan Setiausaha Bahagian, Bahagian Pengurusan Maklumat

.....
(Setiausaha Bahagian, Bahagian Pegurusan Maklumat)
b.p. Setiausaha Kerajaan Negeri Selangor

Tarikh : .....

Lampiran 2

Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT PEJABAT SUK SELANGOR



Lampiran 3

SENARAI PERUNDANGAN DAN PERATURAN

a. Arahan Keselamatan,

b. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”,

c. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS),

d. Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 bertajuk “Pengurusan Laman Web Agensi Sektor Awam”;

e. Garis Panduan Penerapan Etika Penggunaan Media Sosial Dalam Sektor Awam (MAMPU);

f. Surat Pekeliling Am Bilangan 3 Tahun 2015 bertajuk “Garis Panduan Permohonan Kelulusan Teknikal Dan Pemantauan Projek ICT Agensi Sektor Awam”;

g. Surat Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2015 bertajuk “Panduan Pelaksnaaan Program Turun Padang Sektor Awam”;

h. Surat Arahan KPPA Tindakan Ke Atas Penjawat Awam Yang Mendedahkan/Membocorkan Dokumen/Maklumat Terperingkat Kerajaan bertarikh 28 Januari 2015;

i. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT),

j. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan”,

k. Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk – “Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam”;

l. Akta Tandatangan Digital 1997,

m. SPA Bil. 4 Tahun 2006,

n. Akta Rahsia Rasmi 1972,

o. Akta Jenayah Komputer 1997,

p. Akta Hak cipta (Pindaan) Tahun 1997,

q. Akta Komunikasi dan Multimedia 1998,

r. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama)- “Tatacara Penyediaan, Penilaian dan PenerimaanTender”,

s. Surat Pekeliling Perbendaharaan Bil. 3/1995 –“Peraturan Perolehan Perkhidmatan Perundingan”,

t. Surat Pekeliling Am Bil. 4 Tahun 2006 – “Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam”,

u. Perintah-Perintah Am,

Lampiran 3

SENARAI PERUNDANGAN DAN PERATURAN

v. Arahan Perbendaharaan,

w. Arahan Teknologi Maklumat 2007,

x. Surat Akujanji,

y. MPK Bahagian,

z. myPortfolio, dan

aa. Pelan Kesinambungan Perkhidmatan.

bb. Garis Panduan Penggunaan Mel Elektronik Pejabat SUK Selangor

cc. Prosedur dan Garis Panduan ISMS

dd. Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam bertarikh 24 November 2010;

ee. Surat Arahan MAMPU.702-1/1/7 Jld. 3 (48) bertarikh 23 Mac 2009 bertajuk “Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-agensi Kerajaan”;

ff. Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 bertajuk “Penggunaan Media Jaringan Sosial di Sektor Awam”;

gg. Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 bertajuk “Tatacara Pengurusan Aset Alih Kerajaan (TPA)”;

hh. Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 bertajuk “Panduan Pengurusan Pejabat bertarikh 30 April 2007”; dan

ii. Prosedur Pengurusan Pelaporan Dan Pengendalian Insiden Keselamatan ICT SUK SELANGOR.

jj. Surat Pekeliling AM Bilangan 4 Tahun 2024 bertajuk "Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam"

GARIS PANDUAN PENGGUNAAN DAN PENGURUSAN E-MEL PEJABAT SETIAUSAHA KERAJAAN NEGERI SELANGOR

BAHAGIAN PENGURUSAN MAKLUMAT, PEJABAT SETIAUSAHA KERAJAAN NEGERI SELANGOR

ISI KANDUNGAN

1. PENGENALAN

Mel elektronik atau e-mel adalah merupakan aplikasi yang membolehkan pengguna berkomunikasi antara satu dengan lain dalam bentuk mesej elektronik. Setiap penjawat awam mempunyai e-mel rasmi yang digunakan untuk tujuan rasmi dan didaftarkan di bawah agensi Kerajaan. E-mel rasmi boleh dibahagikan kepada dua kategori iaitu e-mel rahsia rasmi dan e-mel bukan rahsia rasmi.

(a) E-mel Rahsia Rasmi

E-mel yang mengandungi maklumat atau perkara rahsia rasmi yang mesti diberi perlindungan untuk kepentingan keselamatan yang dikelaskan mengikut pengelasannya sama ada *Terhad* atau *Sulit*. Maklumat *Rahsia* atau *Rahsia Besar* TIDAK boleh dihantar melalui e-mel.

(b) E-mel Bukan Rahsia Rasmi

E-mel yang tidak mengandungi maklumat atau perkara rahsia rasmi.

Semua warga Pejabat Setiausaha Kerajaan Negeri Selangor (PSUKSEL) diberi kemudahan e-mel mengikut kelayakannya. Setiap warga adalah bertanggungjawab kepada e-mel masing-masing dan perlu mematuhi etika seperti yang dinyatakan dalam PKPA Bil.1 Tahun 2003 Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik Di Agensi-agensi Kerajaan.

E.4 Tujuan

Tujuan Garis Panduan Penggunaan dan Pengurusan E-mel adalah untuk:

(a) Menerangkan dengan lebih terperinci tatacara penggunaan dan pengurusan e-mel kepada semua pegawai dan kakitangan PSUKSEL;

(b) Memastikan kemudahan e-mel PSUKSEL digunakan dengan baik dan selamat;

(c) Meminimumkan sebarang permasalahan berkaitan penggunaan perkhidmatan e-mel.

E.4 **Skop**

Skop garis panduan ini meliputi:

(a) Kemudahan yang disediakan untuk pengguna e-mel PSUKSEL;

(b) Penggunaan e-mel; dan

(c) Pengurusan rekod-rekod e-mel.

E.4 **Pengguna**

Dokumen ini disediakan khas untuk rujukan dan kegunaan warga kerja Pejabat Setiausaha Kerajaan Negeri Selangor (PSUKSEL) supaya lebih memahami dan seterusnya mengamalkan penggunaan dan pengurusan e-mel yang baik dan efisien. Penggunaan garis panduan ini adalah tertakluk kepada Dasar Keselamatan ICT (DKICT) PSUKSEL yang berkuat kuasa.

2. KEMUDAHAN YANG DISEDIAKAN UNTUK PENGGUNA E-MEL PSUKSEL

E.4 **Hak Milik**

Sistem e-mel PSUKSEL adalah di selenggara oleh Bahagian Pengurusan Maklumat (BPM). Semua akaun e-mel rasmi yang diwujudkan oleh BPM untuk pegawai dan kakitangan adalah merupakan hak milik Bahagian Pengurusan Maklumat. Ia adalah kemudahan yang tertakluk kepada peraturan BPM dan boleh ditarik balik jika penggunaannya melanggar peraturan.

E.4 **Tanggungjawab Pengguna**

Semua pengguna adalah bertanggungjawab ke atas e-mel masing-masing. BPM tidak akan bertanggungjawab ke atas sebarang kesalahan jenayah dan seumpamanya berkaitan e-mel.

E.4 **Permohonan Akaun Baru**

Pentadbir E-mel akan memproses Borang Pengurusan E-mel yang lengkap dan mewujudkan akaun e-mel dalam tempoh tujuh (7) hari bekerja. Pengguna baru mesti menukar kata laluan sementara yang diberikan. ***Panduan Menukar Kata laluan E-mel disertakan sebagai Lampiran A.***

E.4 **Saiz *Mailbox***

Setiap pengguna diberikan *mailbox* bersaiz maksimum 100GB mengikut gred/deskripsi tugas. Setiap pengguna bertanggungjawab untuk menguruskan e-mel masing-masing bagi memastikan e-mel yang disimpan tidak melebihi saiz *mailbox* yang telah diperuntukkan. Sekiranya kapasiti telah digunakan sepenuhnya, e-mel masuk yang baru tidak akan diterima oleh sistem.

E.4 **Fungsi Mengikut Kelayakan**

Akaun e-mel rasmi hanya akan diberikan kepada semua kakitangan atau pengguna yang dibenarkan sahaja yang berjawatan dari Gred 17 dan ke atas. Permohonan akaun e-mel PSUKSEL hendaklah dengan mengisi borang Pengurusan Akaun E-mel yang boleh diperoleh dari Bahagian Pengurusan Maklumat.

Bagi kakitangan Gred 17 ke bawah, kemudahan e-mel akan diberikan tertakluk kepada kelulusan SUB (BPM) mengikut keperluan tugasan rasmi harian.

E.4 **Akaun Yang Tidak Aktif**

Akaun e-mel yang tidak di *login* untuk tempoh 90 hari akan dibekukan penggunaannya dan seterusnya dihapuskan sepenuhnya selepas 30 hari akaun dibekukan kecuali telah dimaklumkan kepada Pentadbir E-mel. Penyelaras ICT Bahagian (sekiranya ada) adalah bertanggungjawab untuk memaklumkan kepada Pentadbir E-mel jika terdapat kakitangan yang telah bertukar/pencen atau berkursus/bercuti panjang. Capaian e-mel kakitangan yang tidak lagi berkhidmat di PSUKSEL akan dihentikan serta-merta.

E.4 **Pemantauan Dan Pemeriksaan Oleh Pentadbir E-mel**

Pentadbir E-mel berhak memasang sebarang jenis perisian atau perkakasan penapisan e-mel yang sesuai untuk mencegah, menapis, menyekat atau menghapuskan mana-mana e-mel yang disyaki mengandungi virus atau berunsur *spamming*. Pentadbir E-mel juga berhak mengakses semua e-mel yang dihantar dan diterima melalui sistem e-mel PSUKSEL bagi tujuan pemeriksaan sekiranya berlaku *security compromise,* aktiviti yang menyalahi undang-undang serta salah tingkah laku dalam penggunaan e-mel.

3. PENGGUNAAN E-MEL

Warga kerja PSUKSEL haruslah menggunakan e-mel secara bertanggungjawab berlandaskan undang-undang negara, peraturan-peraturan Perkhidmatan Awam, Dasar Keselamatan ICT (DKICT) PSUKSEL serta mengikut etika e-mel yang bersopan. Panduan dan etika penggunaan e-mel yang harus diamalkan adalah seperti berikut:

(a) Memastikan penghantaran e-mel rasmi menggunakan akaun e-mel rasmi dan alamat e-mel penerima yang betul;

(b) Segala urusan rasmi adalah dilarang menggunakan alamat e-mel persendirian seperti *yahoo.com*, *gmail.com*, *outlook.com* dan sebagainya;

(c) Mengutamakan penggunaan e-mel sebagai media komunikasi untuk urusan dalaman agensi atau dengan pelanggan luar;

(d) Memastikan setiap e-mel rasmi dibalas dengan kadar segera selewat-lewatnya 1 hari dari tarikh e-mel berkenaan diterima;

(e) Memastikan sebarang mesej yang dihantar melalui e-mel tidak lagi disusuli menerusi media lain seperti faks dan surat;

(f) Memastikan setiap e-mel mempunyai tajuk yang sesuai dengan kandungan e-mel;

(g) Menulis jawapan di bahagian atas mesej e-mel;

(h) Penggunaan huruf besar kandungan e-mel adalah tidak digalakkan dan dianggap tidak beretika. Sebaik-baiknya, gunakan gabungan huruf besar dan huruf kecil;

(i) Menggunakan bahasa dan ayat yang jelas, tepat dan mudah difahami oleh penerima;

(j) Menggunakan bahasa formal di dalam e-mel rasmi;

(k) Menggunakan kemudahan “Reply” untuk menjawab e-mel tanpa sebarang perubahan kandungan asal e-mel;

(l) Memastikan kemudahan "*Reply To All*" digunakan jika jawapan perlu disalin kepada semua penerima e-mel;

(m) Tidak menggunakan kemudahan "*Auto-Reply*" kecuali untuk memaklumkan pegawai lain yang boleh dihubungi sekiranya pegawai berkenaan berada di luar pejabat yang tiada kemudahan Internet;

(n) Menggunakan kemudahan "*Forward*" untuk memanjangkan e-mel kepada penerima lain tanpa sebarang perubahan;

(o) Memastikan kemudahan "salinan kepada" (cc) jika sesuatu e-mel perlu dimaklumkan kepada penerima yang berkaitan sahaja; dan

(p) Memastikan kemudahan "*blind cc*" (bcc) digunakan bagi tujuan khusus dan terkawal (bukan sewenang-wenangnya).

E.4 **Saiz E-mel**

Saiz maksimum e-mel (termasuk kepilan) sama ada untuk dihantar atau diterima adalah 30MB. Jika saiz e-mel adalah agak besar, pengguna disarankan supaya menggunakan kaedah:-

i. inovatif dalam penghantaran fail bersaiz besar seperti menggunakan k aedah muat turun fail dengan memaklumkan lokasi pautan *Uniform Resource Locator* (URL);
ii. pemampatan (*compression*) bagi mengurangkan saiz fail contohnya menggunakan perisian *winrar*.
iii. enkripsi bagi dokumen terperingkat yang dihantar secara elektronik.

E.4 **Enkripsi Fail Kepilan**

Sebarang fail yang dihantar khususnya *Terhad* atau *Sulit* harus dilakukan enkripsi sebelum dikepilkan untuk dihantar kepada penerima bagi menjamin keselamatan dan mengelakkan kebocoran maklumat. Perisian *Desktop Productivity* yang sering digunakan seperti *Microsoft Office* dan *Adobe Acrobat* mempunyai fungsi "*inbuilt*" enkripsi masing-masing. Panduan penggunaan enkripsi perisian tersebut adalah seperti di Lampiran 1. Bagi memperketat lagi keselamatan, pengguna dinasihatkan supaya memaklumkan kata laluan melalui medium yang berasingan. ***Panduan Enkripsi Fail Kepilan disertakan sebagai Lampiran B***

E.4 **Pengimbasan Fail Kepilan**

Pengguna hendaklah sentiasa mengimbas fail yang diterima sebelum membukanya. Pengguna juga hendaklah memastikan fail yang akan dihantar melalui e-mel adalah bebas dari virus.

E.4 **Penerimaan E-mel Tanpa Diminta (*Unsolicited Email*)**

Pengguna seharusnya mengelakkan dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui. Ini bagi melindungi pengguna serta aset ICT PSUKSEL daripada aktiviti yang tidak diingini seperti *phishing*, ancaman virus, *spamming*, dan lain-lain *malware*.

E.4 **Mengenal pasti Identiti Pengguna**

Pengguna perlu mengenal pasti dan mengesahkan identiti pihak yang berkomunikasi dengannya sebelum meneruskan komunikasi dan transaksi maklumat melalui e-mel. Ini bertujuan untuk melindungi maklumat Kerajaan daripada sebarang bentuk penyalahgunaan.

E.4 **Kata laluan**

Kata laluan adalah rahsia dan tidak boleh didedahkan kepada orang lain. Ia disarankan untuk ditukar setiap 6 bulan. Pengguna hendaklah menggunakan kata laluan kukuh yang mempunyai ciri-ciri berikut:

(a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;
(b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau di kompromi;
(c) Panjang kata laluan mestilah **sekurang-kurangnya lapan (8) aksara** dengan gabungan antara **huruf dan nombor (alphanumerik)** dan perlu mengandungi gabungan **huruf besar dan kecil** (contoh: *SUKSelang0r01);*
(d) Kata laluan hendaklah diingat dan tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun;
(e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;
(f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;
(g) Disarankan membuat pertukaran kata laluan semasa atau selepas *login* kali pertama, atau selepas kata laluan diset semula;
(h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;
(i) Mengelakkan penggunaan semula kata laluan yang baru digunakan.

E.4 **Pengesanan Virus**

Pentadbir E-mel hendaklah dimaklumi segera sekiranya disyaki ada serangan virus di mana pengguna menerima mesej dari sistem mengenai *bounced mail* yang pengguna sendiri tidak hantar.

E.4 **Perkara Yang Dilarang Dalam Penggunaan E-mel**

Pengguna adalah dilarang daripada melakukan sebarang aktiviti berikut :-

(a) Menggunakan e-mel untuk menghantar bahan-bahan yang salah di sisi undang-undang seperti bahan lucah, perjudian, jenayah, cetak rompak atau apa-apa maklumat yang menjejaskan reputasi PSUKSEL dan Perkhidmatan Awam;

(b) Menggunakan e-mel rasmi untuk tujuan peribadi, komersial atau politik;

(c) Menghantar e-mel sampah (*junk mail*) dan e-mel *spam*;

(d) Menyebarkan kod perosak seperti *virus*, *worm*, dan *trojan horse* yang boleh merosakkan sistem komputer dan maklumat pengguna lain;

(e) Menyimpan dan memuat turun bahan yang mempunyai hak cipta, termasuk yang dimuat turun dari Internet ke dalam sistem e-mel PSUKSEL atau menyebarkan kepada pihak lain tanpa mendapat kebenaran terlebih dahulu daripada pemilik hak cipta yang berkenaan;

(f) Menggunakan akaun milik orang lain, berkongsi akaun atau memberi akses akaun kepada orang lain untuk menjawab e-mel bagi pihaknya; dan

(g) Menggunakan identiti palsu atau menyamar sebagai penghantar maklumat yang sah.

4. PENGURUSAN REKOD-REKOD E-MEL

Rekod elektronik rasmi adalah merupakan rekod awam mengikut tafsiran Akta Arkib Negara Malaysia No. 44/1996. Ia merangkumi sebarang mesej atau rekod komputer (termasuk fail kepilan) yang diwujudkan, dihantar, diserah, dijawab, diedarkan, disimpan, disalin, dipapar, dibaca atau dicetak oleh sistem atau perkhidmatan sesebuah agensi kerajaan. Rekod awam merupakan sumber strategik dan bahan bukti yang perlu diurus secara terkawal, sistematik dan cekap.

4.1 Penyimpanan Rekod-Rekod E-mel

Pengguna hendaklah mengurus dan memastikan jumlah e-mel yang disimpan di dalam *mailbox* adalah tidak melebihi ruang storan yang telah diperuntukkan dan mengutamakan penyimpanan e-mel yang rasmi dan perlu sahaja. Pengguna disarankan supaya mewujudkan *sub folder* mengikut subjek terutamanya bagi *folder Inbox* dan *folder Sent* untuk menyimpan e-mel. Ini akan memudahkan carian dan mendapatkan kembali sesuatu e-mel.

4.2 Mencetak dan Memfailkan Rekod E-mel

Rekod e-mel berkaitan sesuatu keputusan penting atau tindakan yang telah diambil hendaklah dicetak dan difailkan juga.

4.3 Penghapusan Rekod E-mel

Pengguna hendaklah menghapuskan sebarang e-mel yang berunsurkan e-mel *spam* yang berkemungkinan mempunyai virus. Lain-lain e-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan serta tidak diperlukan lagi juga boleh dihapuskan.

4.4 *Backup* Rekod E-mel

Rekod e-mel penting yang telah berusia melebihi dua (2) bulan dan berkemungkinan besar akan dirujuk semula haruslah di *backup* (*eksport folder*) menggunakan *Microsoft Outlook Personal Folders Backup* iaitu semua data akan disimpan pada *Personal Folders file* (*.pst*) sama ada dalam storan PC atau luaran seperti *pen drive* atau cakera padat (CD). Ini akan mengurangkan penggunaan *mailbox* di samping membuat *backup* sebagai langkah keselamatan. ***Panduan Backup E-mel disertakan sebagai Lampiran C***

5. TANGGUNGJAWAB PENGGUNA

Peraturan penggunaan dan pengurusan e-mel PSUKSEL ini adalah merupakan peraturan yang menggariskan tatacara penggunaan dan pengurusan rekod-rekod e-mel PSUKSEL. Semua pengguna e-mel PSUKSEL hendaklah mematuhi garis panduan ini.

6. KHIDMAT NASIHAT

Sebarang kemusykilan yang timbul berkaitan dengan garis panduan ini hendaklah dirujuk kepada:-

Pentadbir E-mel
Unit Pusat Data,
Bahagian Pengurusan Maklumat,
Tingkat 2 Bangunan SSAAS
40503 Shah Alam

Tel: 03-55447561, Faks: 03-55191189
E-mel: pmel@selangor.gov.my

RUJUKAN

1. Surat Arahan Ketua Pengarah MAMPU rujukan MAMPU.BDPICT.700-2/36(1):

"Pemantapan Penggunaan dan Pengurusan E-mel di Agensi-Agensi Kerajaan" –

MAMPU, 1 Julai 2010.

2. Surat Arahan Ketua Pengarah MAMPU rujukan UPTM159/526/9 Jld.4 (60) : "Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-agensi Kerajaan" – MAMPU, 23 Nov 2007.

3. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 : "Garis Panduan

Mengenai Tatacara Penggunaan Internet Dan E-mel Di Agensi-Agensi Kerajaan" – MAMPU, 2003.

4. "*Malaysian Public Sector Management of Information & Communications Technology Security Handbook* (MyMIS)" – MAMPU, 15 Januari 2002.

5. Garis Panduan Pengurusan Rekod Elektronik: Pengurusan Rekod Elektronik dalam Persekitaran Tidak Berstruktur – Arkib Negara Malaysia, 2003.

6. Rekod Elektronik dan Akta Arkib Negara 2003 – Arkib Negara Malaysia, 2003.

7. Dasar Pengurusan Rekod dan Arkib Elektronik – Arkib Negara Malaysia, 2003.

8. Dasar Keselamatan ICT (PSUKSEL) versi 3.0

GLOSARI

Warga PSUKSEL	Semua kakitangan Pejabat Setiausaha Kerajaan Negeri Selangor
Semua Kakitangan SUK dan PDT	Semua kakitangan Pejabat Setiausaha Kerajaan Negeri Selangor dan Pejabat Daerah dan Tanah Selangor
Pengguna	Semua kakitangan PSUKSEL yang menggunakan perkhidmatan e-mel PSUKSEL.
E-mel	Satu kaedah mengarang, menghantar, menyimpan dan menerima mesej melalui sistem komunikasi elektronik.
E-mel Rasmi	E-mel rasmi adalah merupakan rekod maklumat yang dihasilkan, diterima atau disimpan secara rasmi dengan menggunakan kemudahan elektronik, yang juga tertakluk kepada pentafsiran Rekod Awam. Ini bermaksud mesej e-mel tersebut adalah merupakan maklumat-maklumat atau rekod-rekod yang dihasilkan atau diterima oleh pegawai dan kakitangan PSUKSEL di dalam melaksanakan tugas-tugas rasmi mereka, dan ianya mempunyai kepentingan sebagai bahan bukti kepada sesuatu transaksi itu.
E-mel Tidak Rasmi	E-mel tidak rasmi adalah merupakan rekod e-mel yang dihasilkan, diterima atau disimpan atas urusan peribadi yang dibenarkan oleh PSUKSEL. Ianya tidak mempunyai kaitan langsung dengan tugas-tugas rasmi yang dijalankan oleh pegawai dan kakitangan Perbendaharaan Malaysia.
Mailbox	Peti *mail* pengguna untuk menyimpan semua e-mel yang diterima dan dihantar pengguna.
Rekod	Bahan dalam bentuk bertulis atau bentuk lain yang menyatakan fakta atau peristiwa atau selainnya merakamkan maklumat termasuklah kertas, dokumen, daftar, bahan bercetak, buku, peta, pelan, lukisan, gambar foto, mikrofilem, filem sinematograf, rakaman bunyi, rekod yang dihasilkan secara elektronik, tanpa mengira bentuk atau ciri-ciri fizikal dan apa-apa salinannya.

Rekod Elektronik	Rekod dalam bentuk elektronik atau berdigit yang diwujudkan, ditawan, diselenggarakan atau disimpan semasa menjalankan fungsi Kerajaan selaras dengan takrif rekod yang diberikan dalam Akta Arkib Negara 2003. Ini termasuk tetapi tidak terhad kepada kertas, dokumen, daftar, bahan bermaklumat, buku, peta, pelan, lukisan, gambar foto dan rakaman bunyi dalam bentuk elektronik atau berdigit.
Rekod E-mel	Sebarang mesej atau rekod komputer yang wujud, dihantar, diserah, dijawab, diedar, disimpan, disalin, dipapar, dibaca atau dicetak oleh sistem/perkhidmatan yang menepati istilah Rekod Awam di dalam Akta Arkib Negara 2003.
Rekod Awam	Rekod yang diterima secara rasmi atau yang dikeluarkan oleh mana-mana pejabat awam bagi perjalanan hal ehwalnya atau oleh mana-mana pekhidmat awam atau pekerja pejabat awam dalam perjalanan tugas rasminya dan termasuk rekod mana-mana perusahaan Kerajaan dan juga termasuk segala rekod yang, pada permulaan kuat kuasa Akta ini, adalah dalam jagaan atau di bawah kawalan Arkib Negara Malaysia.

LAMPIRAN

A) Panduan Menukar Kata laluan E-mel

B) Panduan Enkripsi Fail Kepilan (MS Office 2010 / Pro Plus)

C) Panduan Backup E-mel

D) Panduan Konfigurasi E-mel Ke Atas Telefon Bimbit (*IPhone*)

E) Panduan Konfigurasi E-mel Ke Atas Telefon Bimbit (*Android*)

F) Panduan Memindahkan E-mel Yang Sahih Dari Folder *Junk/Spam E-mail*

LAMPIRAN A

A) PANDUAN MENUKAR KATA LALUAN E-MEL

LANGKAH-LANGKAH

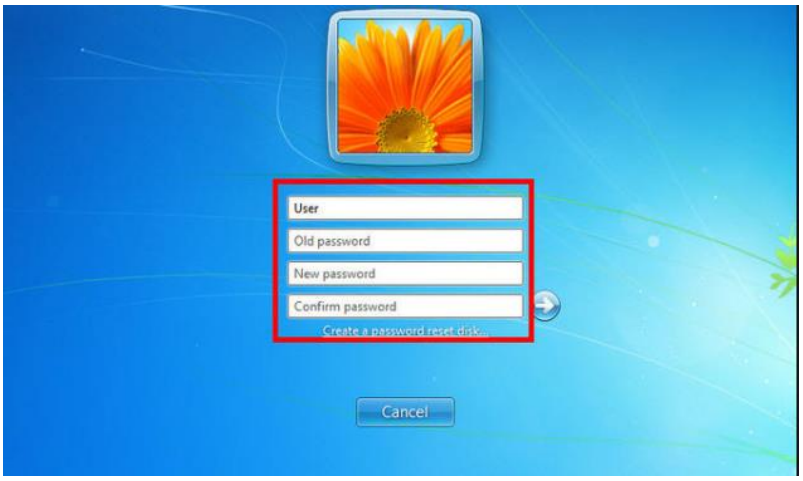
1. Klik ***CTRL + ALT +DEL*** pada papan kekunci komputer.

2. Klik pada ***Change a password.***

3. Masukkan katalaluan lama pada ruangan ***Old password***.

4. Masukkan katalaluan baru pada ruangan ***New password.*** Kata laluan mestilah terdiri daripada sekurang-kurangnya 8 aksara dengan kombinasi alphanumerik (contoh: SUKSelang0r01).

5. Ulangi dengan memasukkan kata laluan yang sama pada ruangan Confirm password.



6. Tekan simbol  untuk meneruskan proses seterusnya.

7. Klik ***Ok*** untuk selesai.

8. Proses kemas kini kata laluan baharu akan mengambil masa selama **30 minit** dan selepas itu barulah pengguna boleh ***login*** ke e-mel menggunakan kata laluan baharu.

LAMPIRAN B

B) PANDUAN ENKRIPSI FAIL KEPILAN (MS OFFICE 2010/MS OFFICE 365 PRO PLUS)

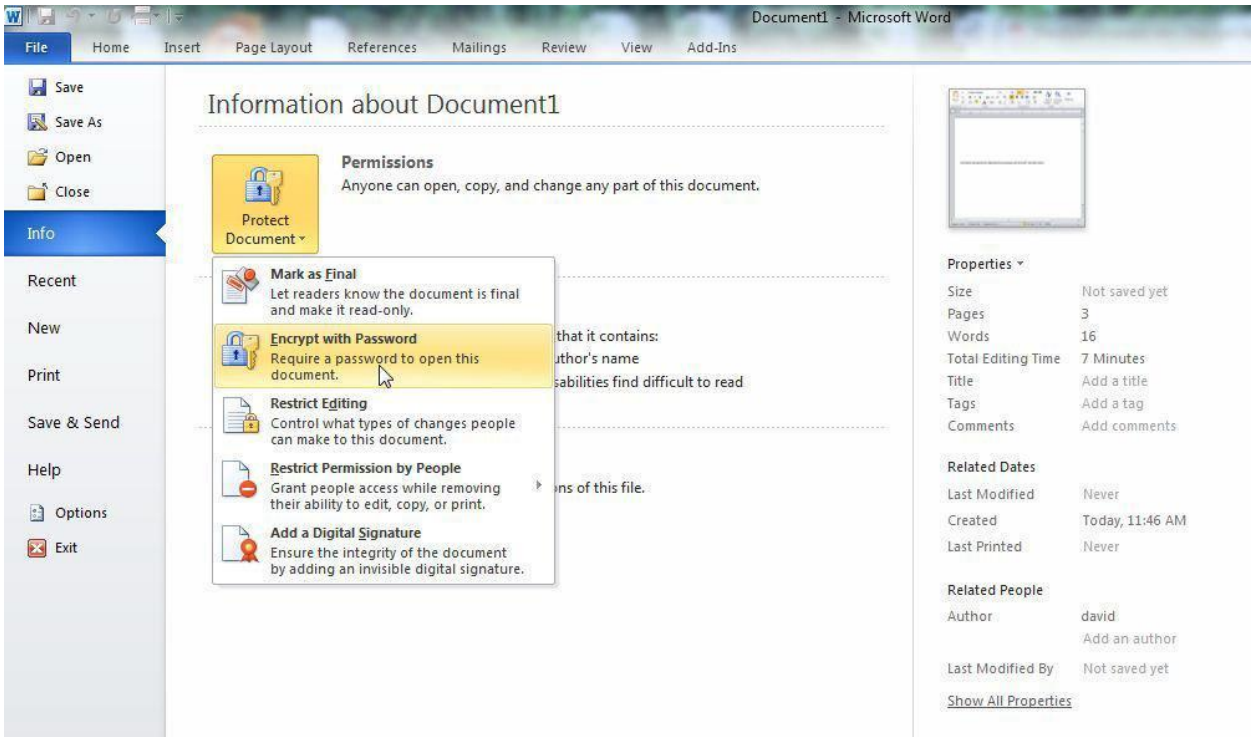
PENGENALAN

Aplikasi ***Microsoft Office*** sering digunakan dalam penghasilan dokumen seharian. Bahagian ini akan menerangkan prosedur enkripsi yang boleh dilakukan pada dokumen berkaitan sebagai langkah keselamatan asas. Selain itu diterangkan juga prosedur penghantaran dokumen enkripsi kepada penerima.

LANGKAH-LANGKAH

1. Buka dokumen (.docx, .xlsx, .pptx) yang hendak dienkrip. Contoh yang ditunjukkan adalah ***Microsoft Word 2010/Microsoft Word Pro Plus***.

2. Buka fail dan pilih ***File>Info>Protect Document>Encrypt*** with ***Password*** seperti Rajah 1.



Rajah 1: Enkripsi/Penyulitan (*Encrypt*) dokumen dalam *Microsoft Word*

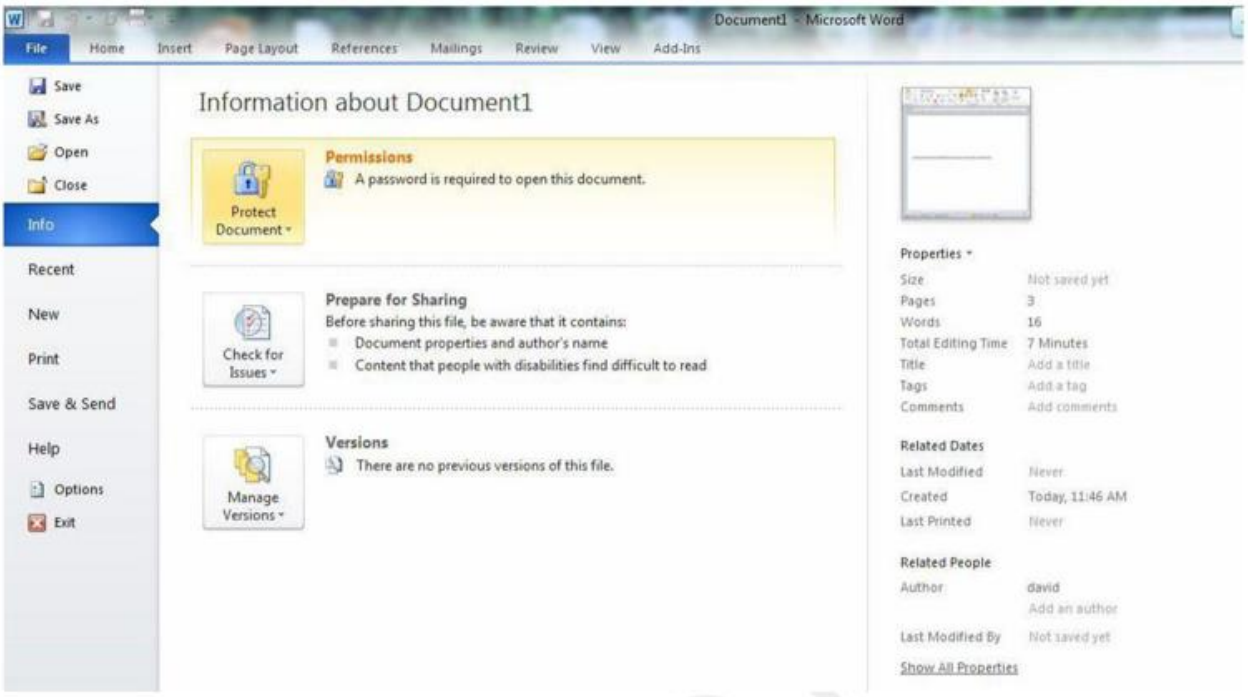
3. Sila masukkan kata laluan yang difikirkan sesuai dan kukuh yang mematuhi Dasar Keselamatan ICT PSUKSEL pada kotak kemasukan kata laluan (Rajah 2) dan klik ***OK*** setelah selesai.

Rajah 2: Penetapan kata laluan untuk membuka dokumen

4. Masukkan kata laluan yang sama pada skrin pengesahan kata laluan yang dipaparkan dan klik ***OK*** setelah selesai.

Rajah 3: Pengesahan kata laluan yang telah dimasukkan

5. Pada skrin yang dipaparkan pada pilihan ***Tab Info***, kelihatan perkataan ***Permissions*** telah bertukar warna menunjukkan enkripsi telah dilaksanakan untuk dokumen ini.



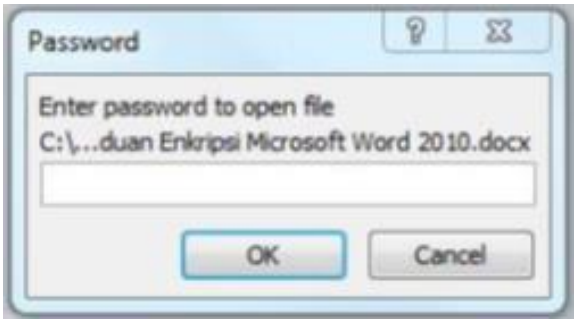
Rajah 4: Perubahan warna teks *Permissions* selepas pelaksanaan enkripsi

6. Sila klik pilihan ***Save Document*** setelah selesai. Ini bagi memastikan penetapan kata laluan dilaksanakan dengan sempurna.

7. Dokumen tersebut kini boleh diedarkan secara elektronik.

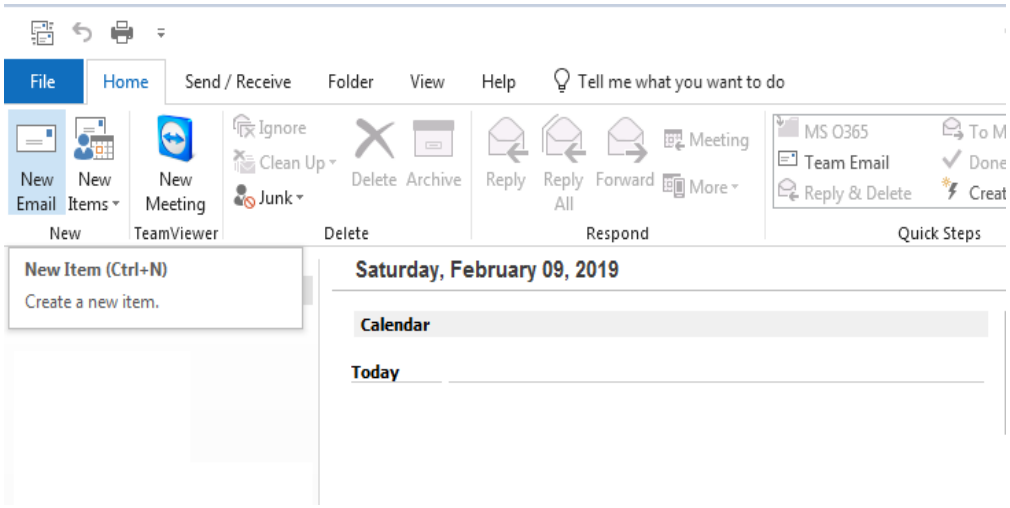
8. Seterusnya, pemilik dokumen akan memaklumkan penerima tentang kata laluan melalui e-mel atau telefon bagi membuka dokumen berkenaan.

9. Dokumen tersebut kini memerlukan kata laluan sebelum boleh dibuka dan/atau diubahsuai oleh penerima (rujuk Rajah 5).



Rajah 5: Keperluan kemasukan kata laluan untuk dokumen yang telah dibuat enkripsi

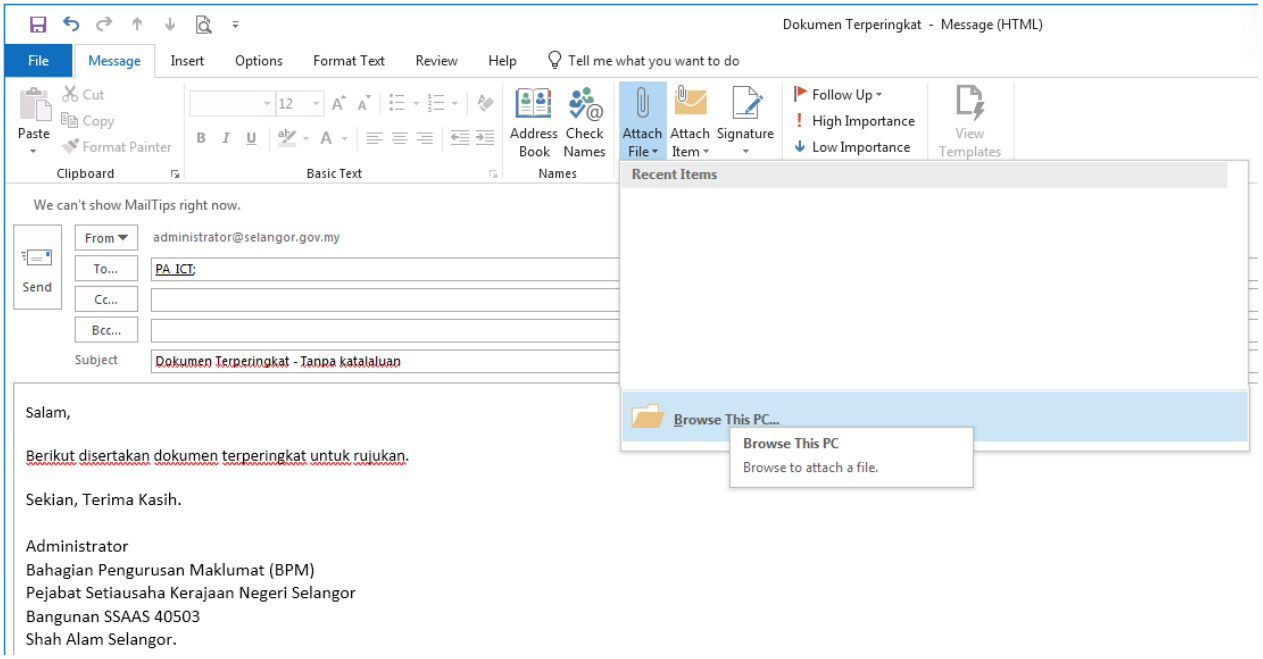
10. Untuk membuat penghantaran dokumen enkripsi melalui e-mel, buka ***MS Office Outlook*** dan klik pada ***New Email*** (rujuk Rajah 6).



Rajah 6: Melalui ***MS Office Outlook*** buka ***New Email*** untuk penghantaran e-mel baru

11. Isikan maklumat penghantaran kepada penerima e-mel (**tanpa dinyatakan kata laluan fail enkripsi**).

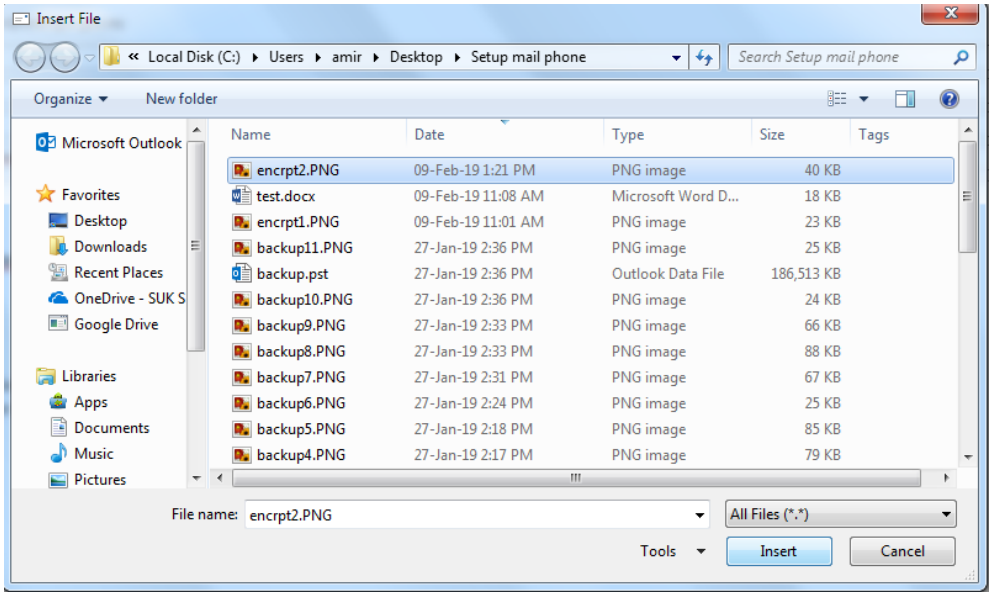
12. Klik pada ***Attach File>Browse This PC*** untuk mencari fail yang disimpan seperti Rajah 7.



Rajah 7: Lampirkan fail enkripsi dalam e-mel yang ingin dihantar

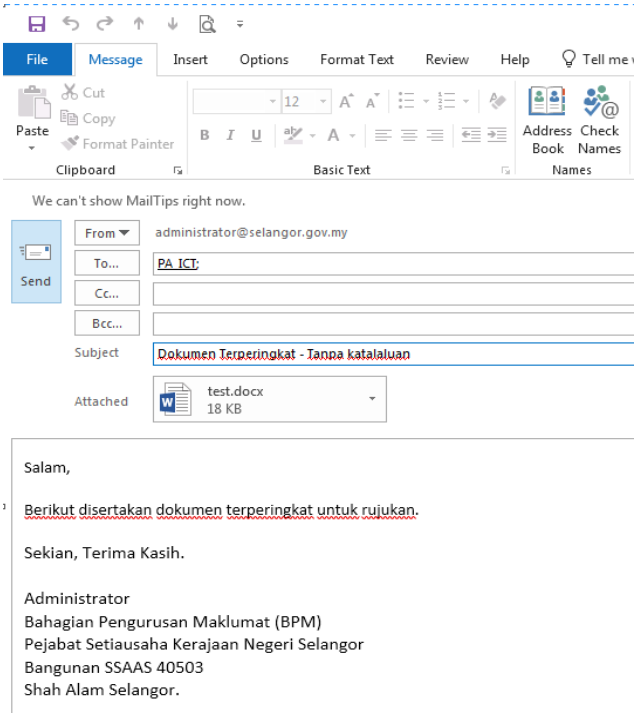
13. Paparan kotak ***Insert File*** akan muncul dan pilih fail enkripsi tersebut.

14. Klik Insert untuk melampirkan fail tersebut ke dalam e-mel seperti Rajah 8.



Rajah 8: Pilihan fail enkripsi untuk dilampirkan pada e-mel

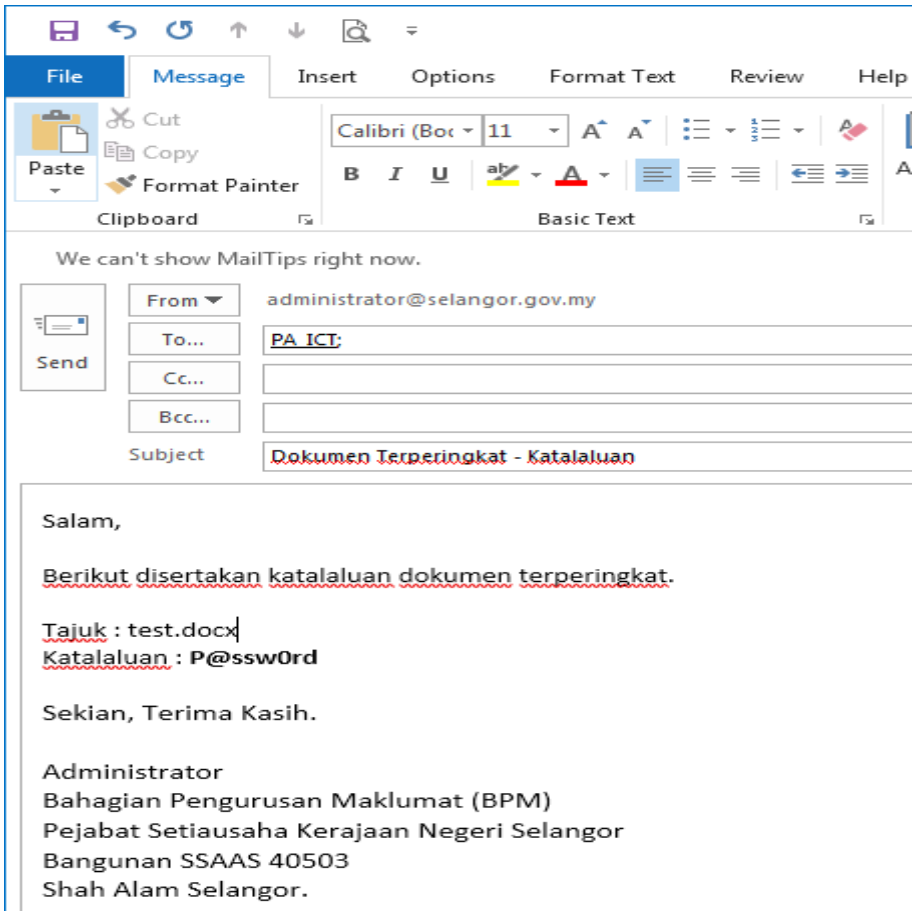
15. Klik ***Send*** untuk menghantar e-mel seperti Rajah 9



Rajah 9: Penghantaran e-mel fail enkripsi

16. Ulangi proses (No.10) untuk membuat penghantaran kata laluan fail enkrispi seperti Rajah 10.

17. Klik ***Send*** untuk menghantar e-mel kepada penerima.



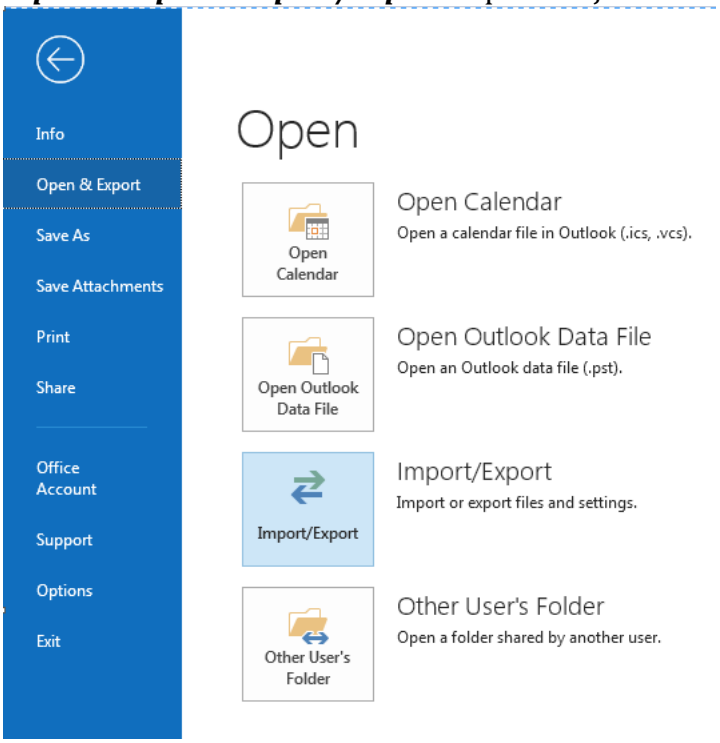
Rajah 10: Penghantaran e-mel kata laluan fail enkripsi

LAMPIRAN C

C) PANDUAN BACKUP E-MEL

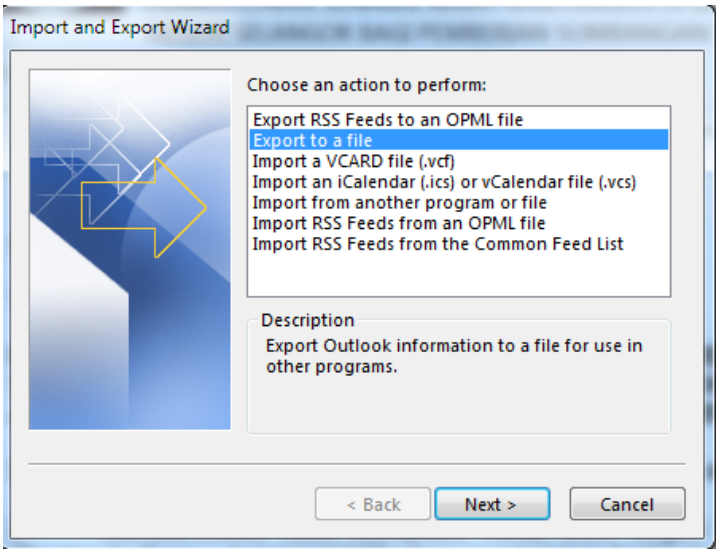
LANGKAH-LANGKAH

1. Buka ***Microsoft Office Outlook***.
2. Pilih ***File>Open & Export>Import/Export*** seperti Rajah 1.



Rajah 1

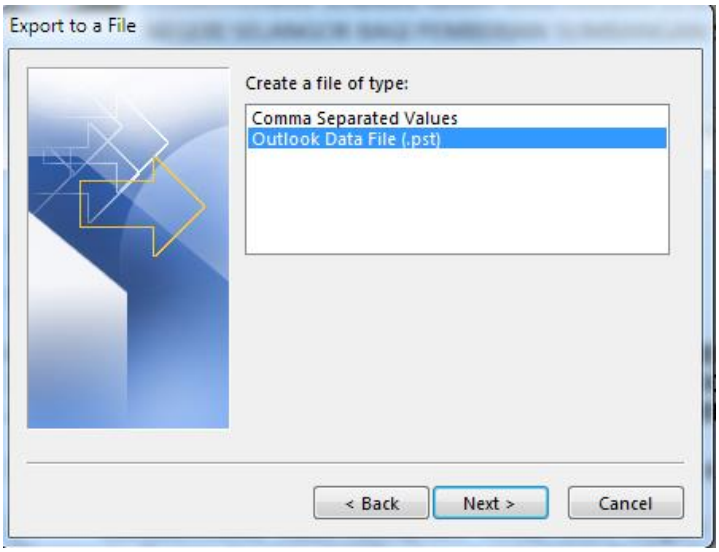
3. Paparan kotak ***Import and Export Wizard*** akan muncul seperti Rajah 2.
4. Pilih ***Export to a file*** dan klik ***Next***.



Rajah 2

5. Paparan kotak ***Export to a file*** akan muncul seperti Rajah 3.

6. Pilih ***Outlook Data File (.pst)*** dan klik ***Next.***

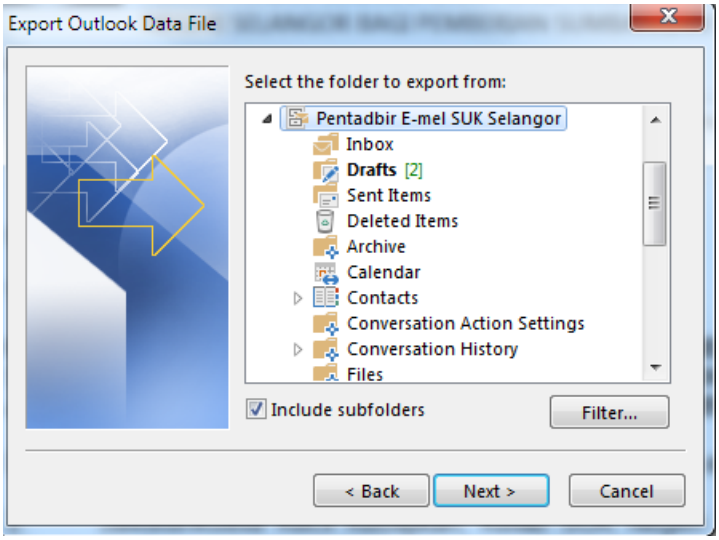


Rajah 3

7. Paparan kotak ***Export Outlook Data File*** akan muncul seperti Rajah 4.

8. Pilih folder yang ingin di buat backup. Sebaiknya semua folder dengan memilih pada folder nama pengguna e-mel.

9. Pastikan tick pada kotak ***Include subfolders*** dan klik ***Next***.



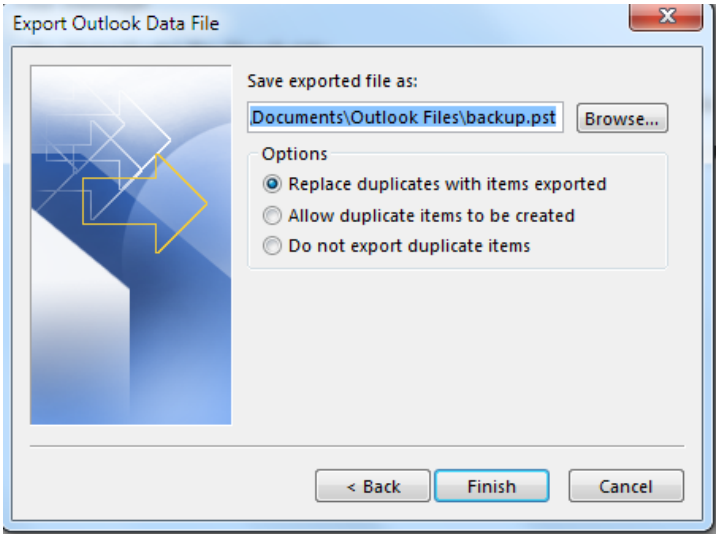
Rajah 4

10. Paparan kotak ***Create Outlook Data File*** akan muncul seperti Rajah 5.

11. Sila masukkan kata laluan yang difikirkan sesuai dan kukuh yang mematuhi Dasar Keselamatan ICT PSUKSEL pada ruangan ***Password*** dan ulangi kata laluan yang sama pada ruangan ***Verify Password*** dan klik Ok.

Rajah 5

12. Paparan kotak ***Export Outlook Data File*** akan muncul seperti Rajah 6.

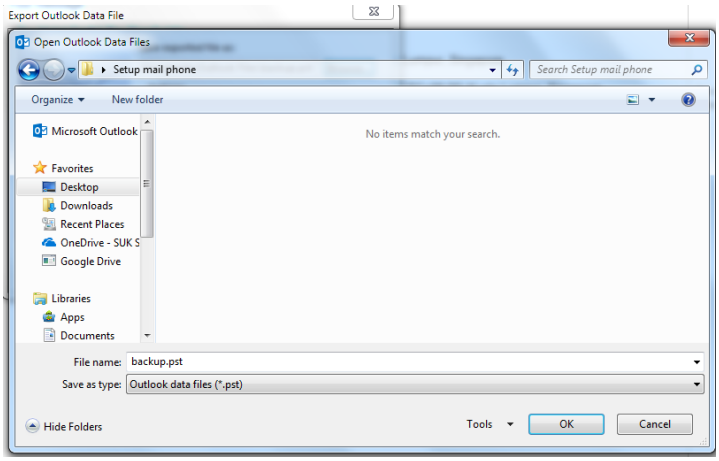


Rajah 6

13. Klik pada ***Browse*** dan paparan akan muncul seperti Rajah 7.

14. Pilih folder yang ingin di simpan fail backup tersebut dan isikan nama fail mengikut kesesuaian.

15. Klik ***Ok***.

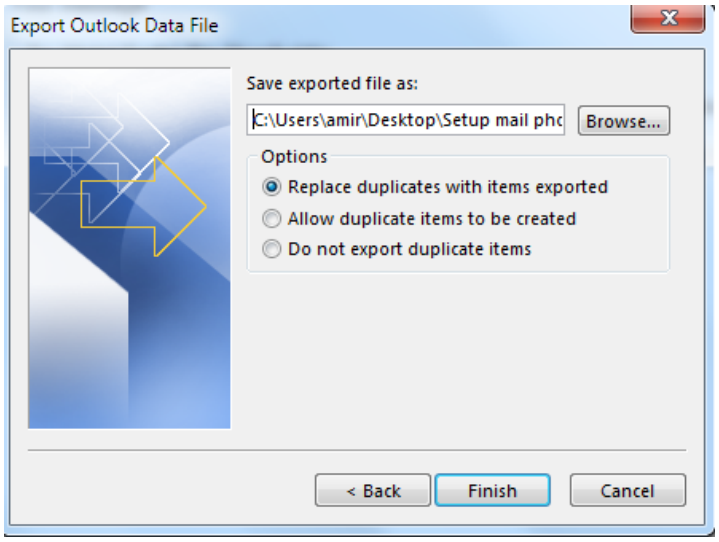


Rajah 7

16. Paparan akan kembali seperti di Rajah 8.

17. Pada ***Options*** pastikan ***tick*** pada ***Replace duplicates with items exported***.

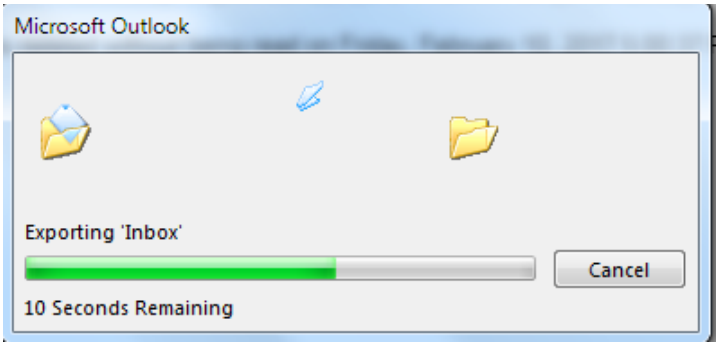
18. Klik ***Finish***.



Rajah 8

19. Paparan akan muncul seperti Rajah 9.

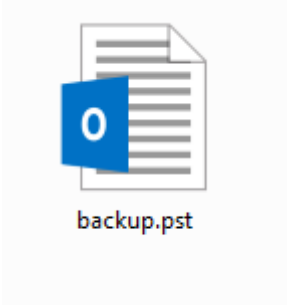
20. Ia menunjukkan proses backup sedang berjalan dan sila tunggu sehingga proses tersebut selesai.



Rajah 9

21. Setelah proses selesai fail ***backup*** tersebut telah berjaya disimpan pada lokasi folder yang dipilih sebelum ini (Rajah 7).

22. Contoh fail yang telah berjaya di ***backup*** adalah seperti Rajah 10.



Rajah 10

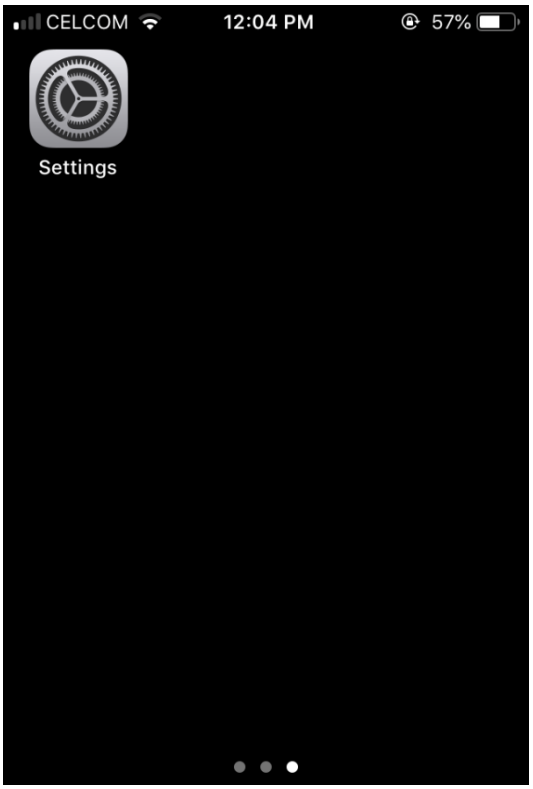
LAMPIRAN D

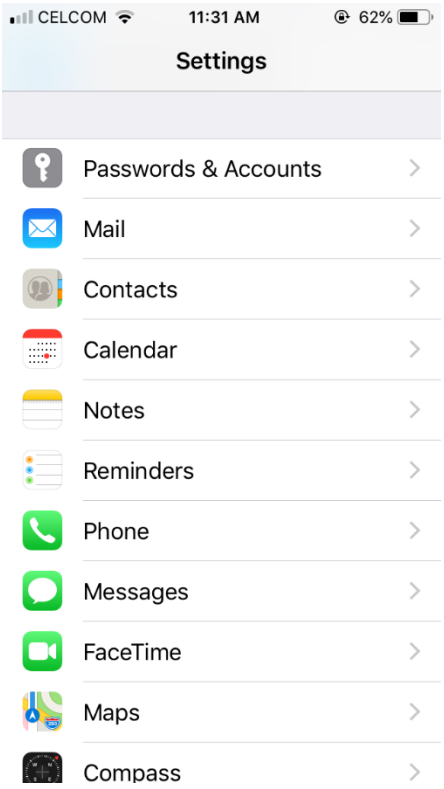
D) PANDUAN KONFIGURASI E-MEL KE ATAS TELEFON BIMBIT (IPHONE)

LANGKAH-LANGKAH

1. Klik pada ikon ***Settings***.

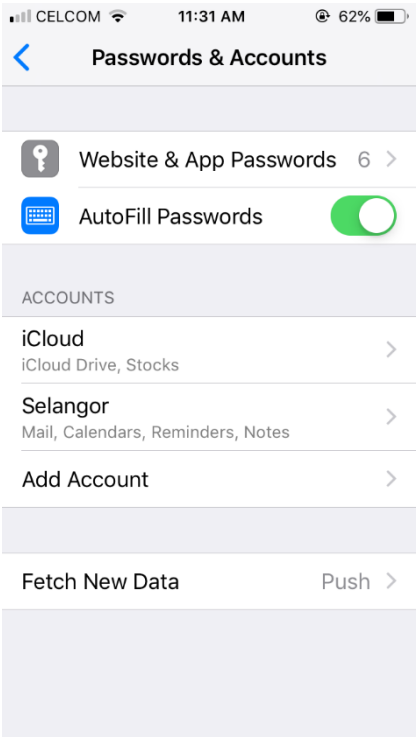
2. Pilih menu ***Passwords & Accounts.***

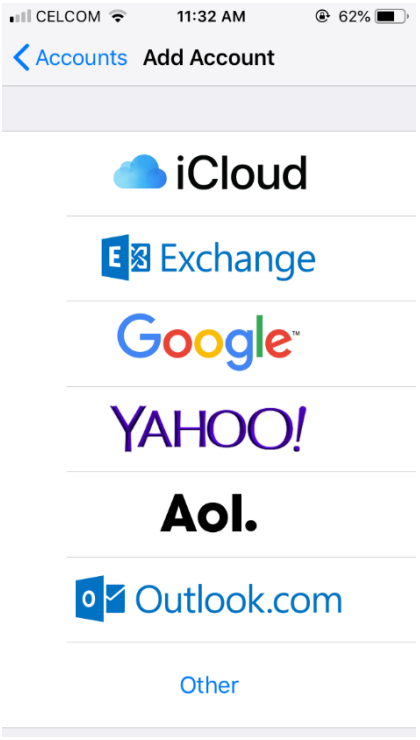




3. Klik ***Add Account.***

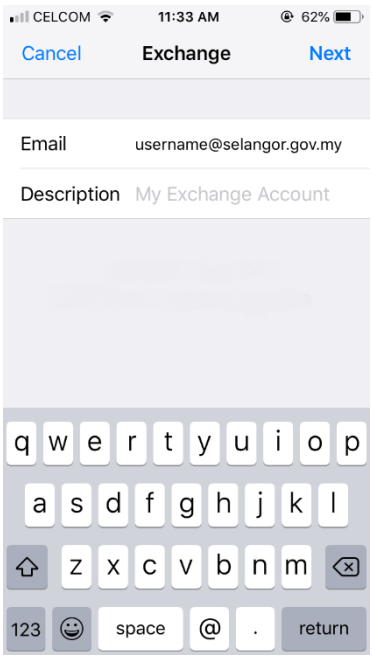
4. Pilih ***Exchange***

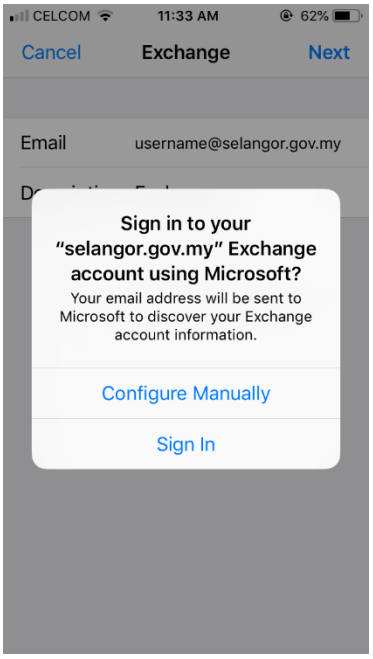




5. Pada ruangan Email taipkan ID E-mel Tuan/Puan dan klik ***Next***.

6. Pilih ***Configure Manually***.

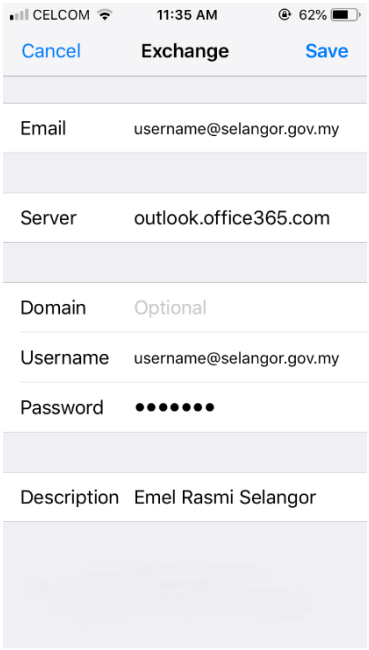


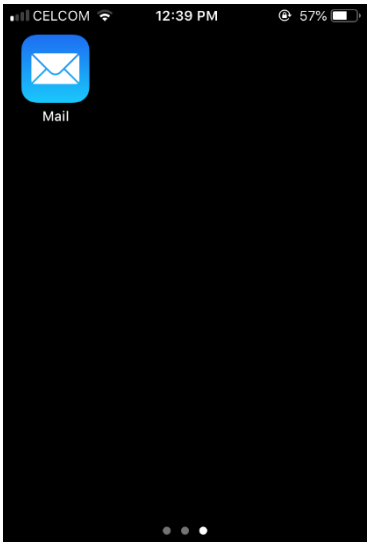


7. Masukkan maklumat yang diperlukan seperti di bawah.

8. Klik **Save**.

9. Klik ikon ***Mail*** untuk akses kepada e-mel.





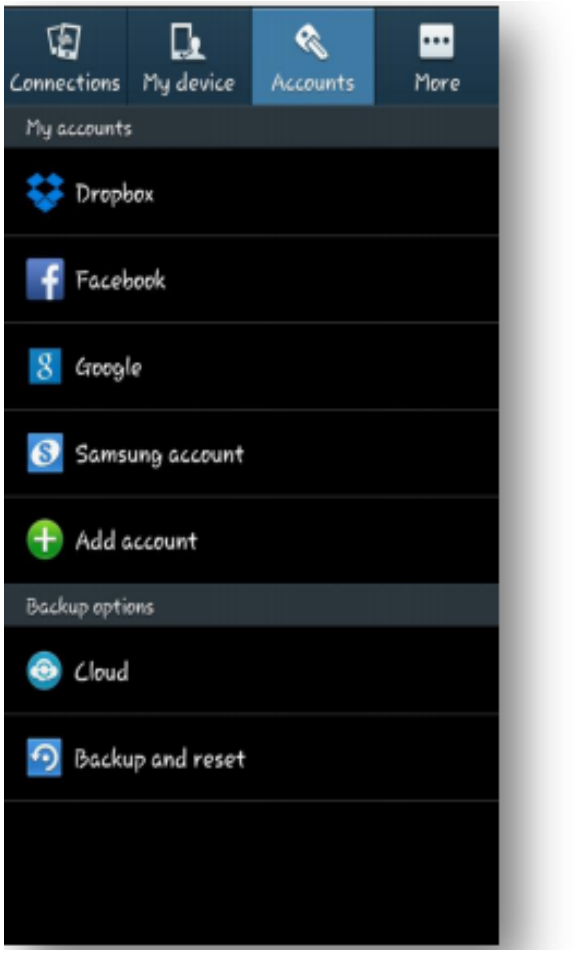
LAMPIRAN E

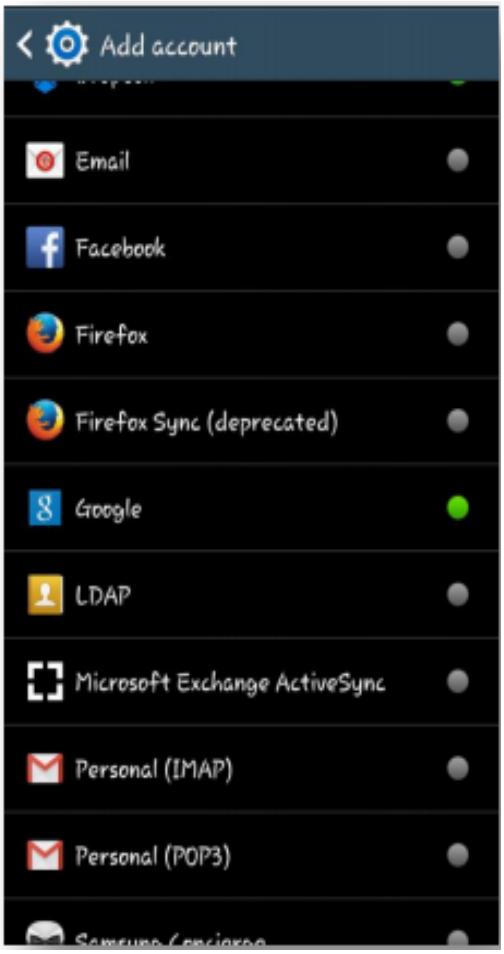
E) PANDUAN KONGFIGURASI E-MEL KE ATAS TELEFON BIMBIT (ANDROID)

LANGKAH-LANGKAH

1. Pilih ***Settings>Accounts>Add account>Microsoft Exchange ActiveSync***

2. Klik ***Next***.





3. Masukkan ***Email address*** (alamat e-mel) dan ***Password*** (katalaluan).

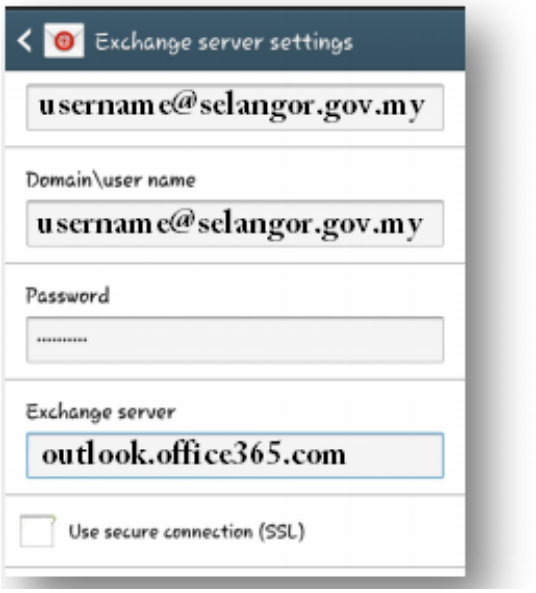
4. Klik ***Manual setup.***

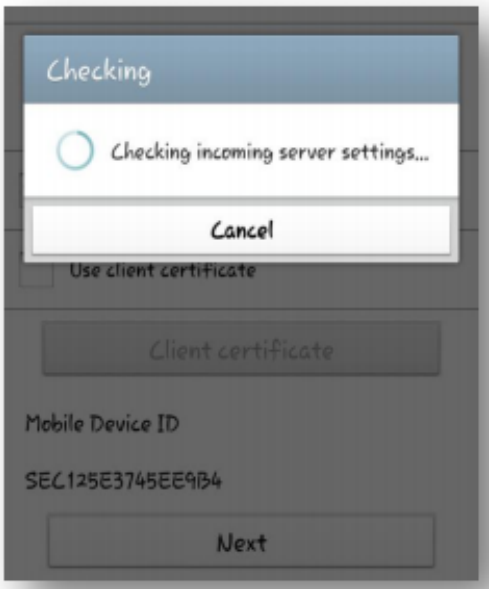
5. Lengkapkan maklumat pada ruangan berikut:

   Domain\username : Masukkan alamat e-mel

   Exchange server : outlook.office365.com

6. Klik ***Next.***

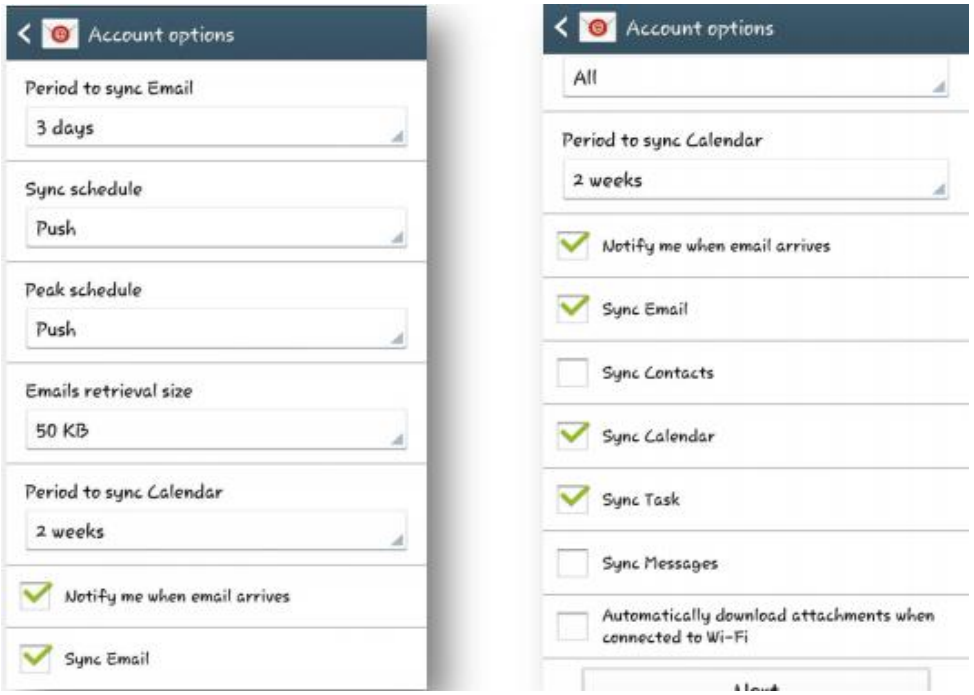




7. Berikut adalah konfigurasi untuk akaun e-mel yang diwujudkan.

   Period to sync Email : Tempoh masa untuk sync e-mel boleh diubah mengikut kesesuaian pengguna.

8. Klik ***Next.***



9. Langkah terakhir adalah untuk menamakan akaun e-mel yang telah di konfigurasi mengikut kesesuaian pengguna.

10. Klik ***Done***.

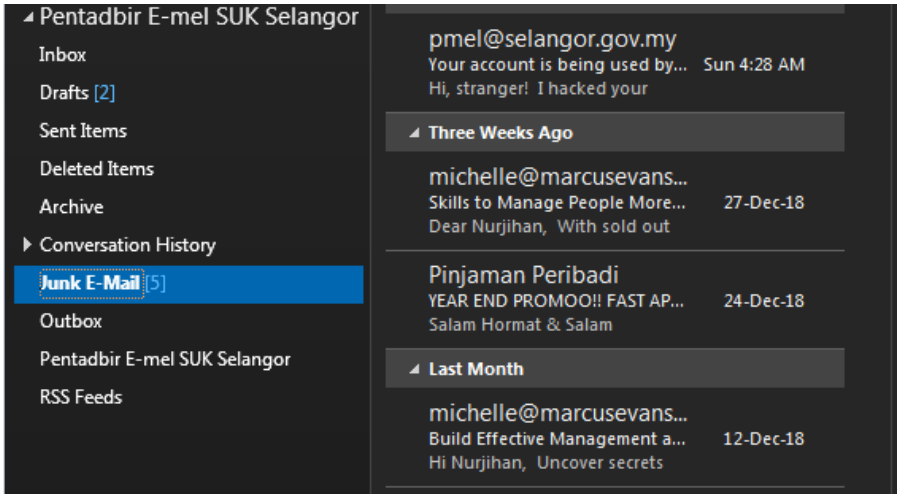
LAMPIRAN F

F) PANDUAN MEMINDAHKAN E-MEL YANG SAHIH DARI FOLDER SPAM/JUNK E-MAIL

LANGKAH-LANGKAH

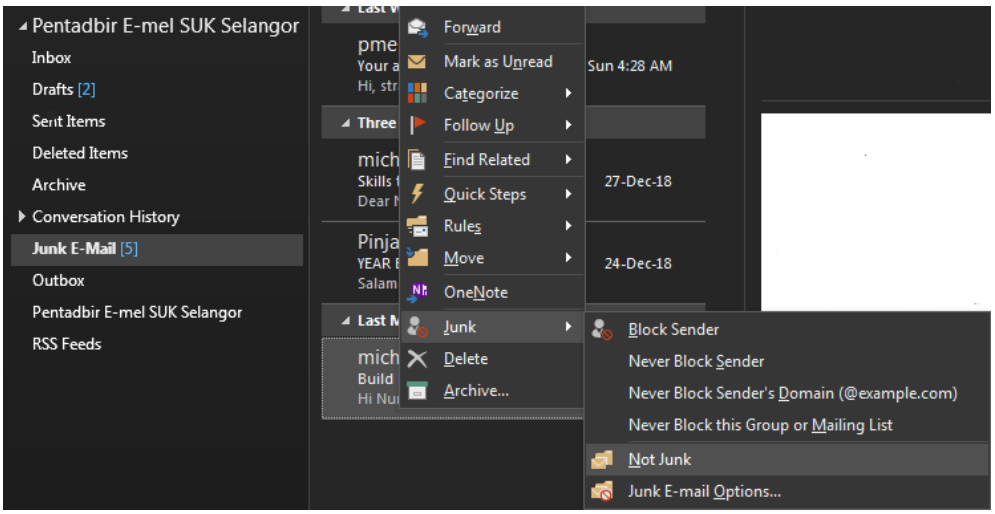
1. Buka e-mel dan pilih ***Junk E-mail.***

2. Semak sekiranya e-mel yang sahih (bukan e-mel SPAM) berada di dalam folder ***Junk E-mail.***



3. Klik butang kanan tetikus (***mouse***) pada e-mel yang sahih.

4. Satu ***pop-up*** akan muncul dan pilih ***Junk>Not Junk*** untuk menukar status e-mel tersebut.



1. Pastikan kotak ditandakan ✓ dan klik ***OK*** untuk pengesahan terakhir bahawa e-mel tersebut diklasifikasikan sebagai e-mel yang sahih.

2. Setelah itu, secara automatik e-mel tersebut akan dipindahkan ke folder ***Inbox*** dan ia tidak lagi akan masuk ke folder ***Junk-Email*** di masa akan datang.