KETUA SETIAUSAHA
KEMENTERIAN KESIHATAN MALAYSIA
Secretary General
Ministry of Health, Malaysia

Aras 12, Blok E7, Kompleks E
Pusat Pentadbiran Kerajaan Persekutuan
62590 Putrajaya
MALAYSIA

Telefon : 03-8883 2539
Web : www.moh.goh.my
Emel : pejabatksu@moh.gov.my

Ruj. Kami : KKM.100-1/6/14 JLD. 2 (8)
Tarikh : 3 Disember 2025

Semua Setiausaha / Pengarah Bahagian
Semua Pengarah Kesihatan Negeri
Semua Pengarah Institut
Semua Pengarah Hospital
Semua Ketua Pegawai Eksekutif Badan Berkanun Persekutuan
Kementerian Kesihatan Malaysia

YBhg. Datuk/ Dato'/Datin/Dr./Tuan/ Puan,

SURAT PEKELILING KETUA SETIAUSAHA
KEMENTERIAN KESIHATAN MALAYSIA BILANGAN 4 TAHUN 2025

PELAKSANAAN POLISI KESELAMATAN SIBER VERSI 1.0
KEMENTERIAN KESIHATAN MALAYSIA

1.0 TUJUAN

Surat pekeliling ini bertujuan untuk menjelaskan pelaksanaan Polisi Keselamatan Siber (PKS) Kementerian Kesihatan Malaysia (KKM) dan perkara-perkara berkaitan yang perlu dipatuhi dalam pengukuhan keselamatan siber Kementerian Kesihatan Malaysia.

2.0 LATAR BELAKANG

2.1 Surat Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan telah dikeluarkan oleh MAMPU pada 1 Oktober 2000. Pekeliling ini dirumus bagi memenuhi keperluan penguatkuasaan, kawalan dan langkah-langkah menyeluruh untuk melindungi aset ICT Kerajaan. Semua agensi Kerajaan dipertanggungjawabkan untuk memastikan dasar keselamatan ICT Kerajaan dilaksanakan dan dipatuhi.

2.2 Sejak itu, Dasar Keselamatan ICT (DKICT) telah menjadi asas kepada pengurusan keselamatan ICT di Kementerian Kesihatan

Malaysia (KKM). DKICT KKM Versi 5.0 telah diluluskan di Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KKM Bilangan 3/2019 bertarikh 2 Ogos 2019.

2.3 Selaras dengan Arahan Majlis Keselamatan Negara (MKN) No.26 Tahun 2017: Perlindungan Infrastruktur Maklumat Kritikal Negara (NCII) serta penubuhan Agensi Keselamatan Siber Negara (NACSA) sebagai penyelaras keselamatan siber nasional, kerajaan telah memperkukuh pendekatan keselamatan ICT kepada pendekatan keselamatan siber menyeluruh yang turut merangkumi perlindungan aset digital, data, dan infrastruktur teknologi.

2.4 Sehubungan dengan itu, Dasar Keselamatan ICT (DKICT) Kementerian Kesihatan Malaysia telah dijenamakan semula sebagai Polisi Keselamatan Siber (PKS) KKM bagi memastikan pengurusan keselamatan siber kementerian selaras dengan dasar nasional, aset, sumber, rekod, infrastruktur, keperluan perundangan dan perkembangan teknologi semasa.

2.5 PKS ini dibangunkan berdasarkan kerangka antarabangsa ISO/IEC 27001:2022 serta mengambil kira obligasi kementerian di bawah Akta Keselamatan Siber 2024 (Akta 854). Pelaksanaan PKS ini bertujuan memperkukuh ketahanan siber kementerian dan memastikan semua pengguna mematuhi garis panduan, prinsip dan kawal selia yang ditetapkan.

3.0 POLISI KESELAMATAN SIBER KEMENTERIAN KESIHATAN MALAYSIA

Polisi Keselamatan Siber (PKS) KKM Versi 1.0 seperti di Lampiran A telah diluluskan di Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KKM Bilangan 10/2025 bertarikh 22 Oktober 2025. Polisi ini adalah terpakai kepada semua pengguna di Kementerian termasuk kakitangan, kontraktor, pembekal, dan pakar runding yang terlibat dalam pengurusan, pemprosesan, capaian, perkongsian, penyimpanan dan penyelenggaraan aset digital serta sistem maklumat KKM.

4.0 TANGGUNGJAWAB AGENSI DI BAWAH KKM

4.1 Setiap Ketua Bahagian/Jabatan di bawah Kementerian Kesihatan Malaysia hendaklah memastikan pelaksanaan Polisi Keselamatan Siber (PKS) ini di peringkat masing-masing serta memantau pematuhannya secara berterusan. Sebarang ketidakpatuhan boleh menjejaskan keselamatan aset digital dan maklumat kementerian.

4.2 Sistem ePatuh KKM yang sedang digunapakai ketika ini dihentikan penggunaannya berkuatkuasa 1 Januari 2026. Sistem ePatuh sedia ada kini sedang melalui proses naik taraf secara berperingkat bagi menyokong keperluan dan kawal selia di bawah Polisi Keselamatan Siber (PKS) yang baharu. Sebarang penyelarasan teknikal, modul tambahan atau penyesuaian rekod pematuhan akan dimaklumkan setelah proses pembangunan dimuktamadkan.

5.0 TARIKH KUAT KUASA

Surat Pekeliling ini berkuat kuasa mulai tarikh ia dikeluarkan.

6.0 PEMBATALAN

Dengan berkuatkuasanya Surat Pekeliling ini, maka Surat Pekeliling KSU KKM Bilangan 10 Tahun 2019 – Dasar Keselamatan ICT Versi 5.0 Kementerian Kesihatan Malaysia adalah dibatalkan.

Sekian, terima kasih.

"MALAYSIA MADANI"

"BERKHIDMAT UNTUK NEGARA"

Saya yang menjalankan amanah,

(DATO' SRI SURIANI BINTI DATO' AHMAD)
Ketua Setiausaha
Kementerian Kesihatan Malaysia

Salinan Kepada:

Ketua Pengarah Kesihatan

Timbalan Ketua Setiausaha (Pengurusan)

Timbalan Ketua Setiausaha (Kewangan)

Timbalan Ketua Pengarah Kesihatan (Perubatan)

Timbalan Ketua Pengarah Kesihatan (Kesihatan Awam)

Timbalan Ketua Pengarah Kesihatan (Penyelidikan dan Sokongan Teknikal)

Timbalan Ketua Pengarah Kesihatan (Kesihatan Pergigian)

Timbalan Ketua Pengarah Kesihatan (Perkhidmatan Farmasi)

Timbalan Ketua Pengarah Kesihatan (Keselamatan dan Kualiti Makanan)

LAMPIRAN A

(Flipbook)

MOH/T/BKP/3.25(BK)

KEMENTERIAN KESIHATAN MALAYSIA



POLISI KESELAMATAN SIBER

VERSI 1.0

KESELAMATAN DIGITAL TANGGUNGJAWAB BERSAMA

@ Kementerian Kesihatan Malaysia 2025
ISBN 978-967-2469-83-4
Hak cipta terpelihara. Tiada bahagian terbitan ini boleh diterbitkan semula atau ditukar dalam apa jua bentuk dengan apa jua cara sama ada elektronik, mekanikal, fotokopi, rakaman dan sebagainya tanpa kebenaran bertulis daripada Ketua Setiausaha Kementerian Kesihatan Malaysia.

Cetakan Pertama 2025

Diterbitkan oleh:
Kementerian Kesihatan Malaysia
Blok E1, E3, E6, E7 & E10, Kompleks E
Pusat Pentadbiran Kerajaan Persekutuan
62590 Putrajaya, Malaysia.
Portal: www.moh.gov.my

Dicetak Oleh:
SUNSHOWER VENTURES SDN BHD
No. 187-1, Jalan LP 7/2, Kinrara Uptown,
43300 Seri Kembangan, Selangor.
Tel: +60123071166

KEMENTERIAN KESIHATAN MALAYSIA

POLISI KESELAMATAN SIBER

VERSI 1.0

KESELAMATAN DIGITAL TANGGUNGJAWAB BERSAMA

SEJARAH DOKUMEN

BIL	VERSI	KELULUSAN	TARIKH KUATKUASA
1.	1.0	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) Kementerian Kesihatan Malaysia (KKM) Bilangan 10/2025 -Polisi Keselamatan Siber (PKS) Kementerian Kesihatan Malaysia Versi 1.0	22 Oktober 2025

REKOD PINDAAN

TARIKH	VERSI	KELULUSAN
22 Oktober 2025	1	Polisi Keselamatan Siber diangkat dan diluluskan dalam Mesyuarat Jawatankuasa Pemandu ICT Kementerian Kesihatan Malaysia (KKM) Bilangan 10/2025

GLOSARI

ISTILAH	TAKRIF
Ancaman	Ancaman (Threat) dalam konteks keselamatan maklumat dan siber merujuk kepada sebarang potensi bahaya yang boleh menyebabkan kemudaratan kepada aset, data, sistem, atau operasi organisasi. Ancaman boleh datang dalam pelbagai bentuk dan boleh dieksploitasi oleh penyerang untuk mendapatkan capaian yang tidak sah, mencuri maklumat, mengganggu operasi, atau menyebabkan kerosakan kepada sistem.
Antimalware	Perisian yang direka untuk melindungi sistem komputer dan rangkaian daripada perisian hasad (perisian hasad).
Antivirus	Perisian keselamatan yang berfungsi untuk mengimbas, mengesan, menghalang dan membuang perisian hasad (malware) termasuk virus dan lain-lain ancaman keselamatan dari sistem komputer, media storan atau rangkaian.
Aset	Sebarang komponen bernilai kepada organisasi yang berkaitan dengan maklumat, termasuk sistem, perisian, perkakasan, data, perkhidmatan, kemudahan, dan kakitangan, yang memerlukan perlindungan bagi menjamin kerahsiaan, integriti dan ketersediaan maklumat.
Aset Alih	Semua harta fizikal milik organisasi yang boleh dialihkan tanpa merosakkan strukturnya, seperti komputer, perabot, peralatan pejabat, dan peranti mudah alih.
BYOD	*Bring Your Own Device (BYOD)* – Bawa Peranti Anda Sendiri Dasar yang membenarkan pengguna menggunakan peranti peribadi seperti komputer riba atau telefon pintar untuk mengakses sistem dan data organisasi dengan kawalan keselamatan tertentu.
BUDR	*Backup and Disaster Recovery (BUDR)* - Pelan Sandaran dan Pemulihan Bencana Pendekatan yang melibatkan penyimpanan salinan data dan perancangan pemulihan sistem bagi memastikan kesinambungan operasi sekiranya berlaku gangguan atau bencana.
CCTV	*Closed-Circuit Television (CCTV)* -Kamera Litar Tertutup Sistem kamera litar tertutup dipasang dalam premis bagi tujuan pemantauan keselamatan fizikal
CDO	*Chief Digital Officer (CDO)* - Ketua Pegawai Digital Ketua Pegawai Digital bertanggungjawab merancang dan melaksana strategi dalam memacu inovasi teknologi digital bagi meningkatkan penyampaian perkhidmatan, mengoptimumkan penggunaan data dan analitik, memastikan keselamatan siber, dan menyelaras perubahan budaya serta pengurusan sumber manusia untuk memastikan organisasi kekal kompetitif dan relevan dalam era digital yang pesat berkembang.
Clear Desk	Amalan menyimpan dokumen sensitif, peralatan ICT, dan bahan sulit apabila tidak digunakan, bagi melindungi maklumat daripada akses fizikal tidak sah.
Clear Screen	Amalan mengunci skrin komputer atau peranti apabila tidak digunakan bagi mengelakkan capaian tidak dibenarkan.
CSIRT IPKKM	*Cyber Security Incident Response Team (CSIRT)* Ibu Pejabat KKM Pasukan Tindak Balas Insiden Keselamatan Siber yang ditubuhkan untuk mengesan, menyelaras, mengurus dan bertindak balas terhadap insiden keselamatan siber di Ibu Pejabat KKM.

ISTILAH	TAKRIF
CSIRT Fasiliti KKM	*Cyber Security Incident Response Team* Fasiliti KKM Pasukan Tindak Balas Insiden Keselamatan Siber yang ditubuhkan untuk mengurus dan mengendali insiden keselamatan siber di fasiliti KKM .
DoS	*Denial of Service (DoS)* Serangan siber yang bertujuan untuk melumpuhkan sistem atau perkhidmatan dengan membanjiri sumbernya menggunakan trafik yang tinggi.
DDoS	*Distributed Denial of Service (DDoS)* Serangan DoS yang dijalankan secara serentak dari pelbagai sumber bagi menjejaskan kebolehcapaian sistem atau rangkaian sasaran.
Encryption	Enkripsi ialah proses menukar data asal kepada bentuk tersulit menggunakan kunci kriptografi bagi melindungi kerahsiaan semasa penyimpanan atau penghantaran.
Firewall	Sistem keselamatan rangkaian yang mengawal trafik masuk dan keluar berdasarkan peraturan yang ditetapkan bagi mencegah akses tidak sah.
Gateway	Peranti atau sistem yang berfungsi sebagai penghubung antara dua rangkaian atau sistem berbeza bagi membolehkan komunikasi data antara keduanya.
Hub	Peranti rangkaian yang berfungsi untuk menghubungkan beberapa peranti dalam satu rangkaian tempatan (LAN) dengan menghantar data ke semua port.
IPKKM	Ibu Pejabat KKM Bahagian/Cawangan/Unit dan fasiliti yang diletakkan secara terus dibawah seliaan Ibu Pejabat KKM di Putrajaya.
ICT	Information and Communication Technology (ICT)- Teknologi Maklumat dan Komunikasi Merujuk kepada sistem, peralatan, perisian, aplikasi dan perkhidmatan yang digunakan untuk mengurus, memproses, menyimpan, menghantar atau menerima maklumat secara elektronik.
ICTSO IPKKM	*ICT Security Officer (ICTSO)IPKKM*- Pegawai Keselamatan ICT Ibu Pejabat KKM Pegawai yang bertanggungjawab melaksanakan polisi keselamatan siber, menguruskan infrastruktur keselamatan, memantau keselamatan, mengesan pencerobohan, menilai ancaman, menguruskan insiden serta melatih pegawai mengenai langkah perlindungan keselamatan dalam memastikan pematuhan kepada undang-undang dan peraturan keselamatan siber di IPKKM.
Insiden Keselamatan	Merujuk kepada sebarang kejadian yang berpotensi mengancam, menjejaskan, atau telah menjejaskan kerahsiaan, integriti atau ketersediaan sistem, maklumat atau infrastruktur organisasi.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
Internet Gateway	Titik kawalan utama antara rangkaian dalaman organisasi dengan Internet yang mengawal dan memantau semua trafik keluar dan masuk, termasuk fungsi keselamatan seperti penapisan kandungan, firewall, antivirus, dan pemantauan aktiviti rangkaian.
IDS	*Intrusion Prevention System (IPS)* Sistem keselamatan rangkaian yang memantau, mengesan, dan secara automatik menyekat trafik yang mencurigakan atau berbahaya daripada memasuki sistem atau rangkaian, berdasarkan peraturan dan corak serangan yang diketahui.

ISTILAH	TAKRIF
IPS	*Intrusion Prevention System (IPS)* Sistem keselamatan rangkaian yang memantau, mengesan, dan secara automatik menyekat trafik yang mencurigakan atau berbahaya daripada memasuki sistem atau rangkaian, berdasarkan peraturan dan corak serangan yang diketahui.
JPICT	Jawatankuasa Pemandu ICT (JPICT) adalah jawatankuasa dalaman yang ditubuhkan di peringkat kementerian, jabatan atau fasiliti KKM bagi menyelaras perancangan, pelaksanaan, pemantauan dan penilaian aktiviti ICT serta memastikan pematuhan terhadap dasar dan pelan strategik ICT KKM.
KSU	Ketua Setiausaha (KSU) adalah pegawai tertinggi perkhidmatan awam di sesuatu kementerian yang berperanan sebagai ketua pentadbir dan penasihat utama kepada Menteri dalam melaksanakan dasar kerajaan serta memastikan pengurusan, tadbir urus dan program kementerian berjalan dengan teratur.
Ketua Jabatan	Seseorang pegawai yang bertanggungjawab terhadap sesuatu kementerian, jabatan, bahagian, institusi, agensi, cawangan atau unit, termasuklah pegawai daripada Kumpulan Pengurusan Tertinggi atau Kumpulan Pengurusan dan Profesional yang diberi kuasa secara bertulis untuk melaksanakan tugas bagi pihak pegawai awam yang bertanggungjawab.
Kerentanan	Kelemahan aset atau kawalan yang boleh dieksploitasi oleh ancaman *(threat)*
KKM	Merujuk kepada struktur organisasi dibawah Kementerian Kesihatan Malaysia (KKM) seperti berikut: i. Ibu Pejabat KKM ii. Jabatan Kesihatan Negeri (JKN) iii. Pejabat iv. Hospital v. Institusi vi. Klinik vii. Makmal viii. Majlis ix. Lembaga; x. Pusat; dan Lain-lain yang berkaitan
Kriptografi	Kaedah untuk menukar data dan maklumat biasa *(standard format)* kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat supaya hanya pihak yang dibenarkan dapat membaca atau mengaksesnya
LAN	*Local Area Network (LAN)* Rangkaian komputer yang menghubungkan peranti dalam kawasan geografi yang terhad — seperti dalam rumah, pejabat, bangunan, atau kampus.
Lewahan	Lewahan/Penduaan (atau lebih) komponen atau fungsi kritikal sistem dengan matlamat meningkatkan kebolehpercayaan sistem, biasanya dalam bentuk sandaran atau *fail-safe*, atau untuk meningkatkan prestasi sistem sebenar.
Log	Tindakan menyimpan log peristiwa yang berlaku dalam sistem komputer, seperti masalah, ralat atau hanya maklumat tentang operasi semasa. Peristiwa ini mungkin berlaku dalam sistem operasi atau dalam perisian lain. Mesej atau entri log direkodkan untuk setiap peristiwa tersebut. Mesej log ini kemudiannya boleh digunakan untuk memantau dan memahami pengendalian sistem, untuk menyahpepijat masalah atau semasa audit. Perkara ini amat penting dalam perisian pelbagai pengguna, untuk mempunyai gambaran keseluruhan pusat operasi sistem.

ISTILAH	TAKRIF
Melahu *(Idle)*	Tempoh semasa peranti tidak digunakan walaupun sedang di log masuk/ terpasang.
NACSA	*National Cyber Security Agency* (Agensi Keselamatan Siber Negara) Agensi pusat yang bertanggungjawab ke atas semua aspek keselamatan siber bagi memantapkan pengurusan keselamatan siber negara.
NC4	"*National Cyber Coordination and Command Centre* (NC4)" berperanan sebagai tempat rujukan dan perhubungan utama berkaitan keselamatan siber negara oleh semua organisasi dalam dan luar negara serta bertanggungjawab dalam mengurus dan memantau ancaman siber terhadap sistem-sistem kritikal negara, memastikan kesiapsiagaan, pelaksanaan tindak balas serta mitigasi insiden keselamatan siber pada peringkat strategik dan taktikal.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Pegawai Aset	Pegawai yang dilantik secara tetap, sementara dan kontrak yang menggunakan perkhidmatan ICT KKM.
Pegawai KKM	Pegawai yang dilantik secara tetap, sementara dan kontrak yang menggunakan perkhidmatan ICT KKM.
Pegawai Kejuruteraan	Pegawai Kejuruteraan bertanggungjawab terhadap semua kemudahan dan peralatan kejuruteraan yang menyokong operasi ICT dan bukan ICT — seperti *Generator Set (Gen-Set)*, *UPS*, Sistem Penghawa Dingin *(HVAC)*, sistem elektrik, *chiller*, pam air, dan utiliti sokongan lain.
Pegawai Penerima Aset	Pegawai yang bertanggungjawab untuk menerima dan memeriksa aset alih yang diterima. bagi aset teknikal, pegawai penerima yang dilantik hendaklah memiliki kepakaran dalam bidang berkaitan.
Pegawai Pengelas	Pegawai awam yang dilantik oleh Menteri, Menteri Besar, Ketua Menteri atau Premier Sarawak, mengikut mana-mana yang berkenaan, melalui suatu perakuan di bawah tandatangannya untuk mengelaskan apa-apa suratan rasmi, maklumat atau bahan sebagai "Rahsia Besar", "Rahsia", "Sulit" atau "Terhad", mengikut mana-mana yang berkenaan, sebagaimana yang ditakrifkan dalam Bab 1 Arahan Keselamatan
Pegawai Rekod	Pegawai yang bertanggungjawab untuk menyelaras perancangan dan pelaksanaan program pengurusan rekod jabatan, aktiviti konsultansi dan latihan, memastikan penjagaan dan pelupusan rekod awam dijalankan mengikut undang-undang, sentiasa berhubung dengan Arkib Negara Malaysia, serta menyelia kerja-kerja pelaksanaan oleh Pembantu Tadbir Rekod/Kerani Fail.
Pelan Kesinambungan Perkhidmatan (PKP)	Pelan Kesinambungan Perkhidmatan (PKP) merujuk kepada pelan atau perancangan pengurusan kesinambungan perkhidmatan. Perancangan ini yang meliputi segala sumber, proses, peranan dan tanggungjawab semua pihak terlibat yang diperlukan sebelum, semasa dan selepas sesuatu gangguan kepada sistem penyampaian perkhidmatan perlu didokumenkan, diuji dan dikaji semula secara berkala dan dilaksanakan apabila berlaku gangguan. Di samping itu, tindakan dilaksanakan untuk segera membaik pulih pelaksanaan fungsi-fungsi normal agensi dalam tempoh yang ditetapkan.
Pembangun Sistem	Pembangun sistem, juga dikenali sebagai pengaturcara atau jurutera perisian, adalah individu yang bertanggungjawab untuk merancang, membangun, menguji, dan mengekalkan sistem perisian. Mereka memainkan peranan penting dalam memastikan bahawa sistem yang dibina berfungsi dengan baik dan memenuhi keperluan pengguna serta organisasi.
Pemilik Aset	Individu atau entiti yang mempunyai tanggungjawab dan kuasa terhadap pengurusan dan perlindungan aset tersebut.

ISTILAH	TAKRIF
Pemilik Sistem	Pemilik Sistem terdiri daripada pegawai yang terlibat dengan sistem yang dibangunkan.
Pengarah Projek	Individu yang bertanggungjawab untuk merancang, melaksanakan, mengawasi, dan menyelesaikan sesebuah projek. Mereka memainkan peranan penting dalam memastikan projek berjalan lancar dan mencapai matlamat yang telah ditetapkan
Pengguna	Bermaksud mana-mana individu yang menggunakan perkhidmatan ICT di KKM.
Pengkomputeran Awan	Teknologi pengkomputeran yang bergantung kepada sumber pengkomputeran seperti pelayan, storan, pangkalan data, rangkaian dan perisian yang boleh dicapai menerusi rangkaian atau Internet.
Pengurusan Infrastruktur Kunci Awam (PKI)	Sistem yang menguruskan kunci kriptografi dan sijil digital untuk memastikan keselamatan data dan komunikasi dalam talian. PKI menggabungkan perisian, teknologi penyulitan, dan perkhidmatan untuk melindungi data daripada diubah, dihapuskan, atau didedahkan tanpa kebenaran
Pengurus ICT	Pegawai yang mengetuai organisasi ICT di Jabatan/ Bahagian/ Fasiliti/ Unit berkaitan ICT.
Pengurus Projek	Individu yang bertanggungjawab untuk merancang, mengatur, dan mengawasi semua aspek sesebuah projek dari awal hingga akhir. Tugas utama bagi memastikan projek disiapkan mengikut jadual yang ditetapkan, dalam lingkungan bajet yang diperuntukkan, dan memenuhi kualiti serta spesifikasi yang telah ditetapkan oleh pihak berkepentingan.
Pengurus Sumber Manusia	Seorang Pengurus Sumber Manusia ialah individu yang bertanggungjawab menguruskan fungsi-fungsi berkaitan sumber manusia dalam sesebuah jabatan. Tugas-tugas termasuk pengambilan pekerja, pembangunan dan latihan staf, pengurusan prestasi, serta memastikan pematuhan kepada undang-undang buruh dan polisi jabatan. Pengurus Sumber Manusia juga memainkan peranan penting dalam menyelesaikan konflik, menguruskan kebajikan pekerja, dan memastikan suasana kerja yang positif dan produktif. Secara keseluruhan, mereka adalah penghubung utama antara pekerja dan pihak pengurusan untuk menyokong pencapaian matlamat jabatan.
Pentadbir Aset	Pentadbir aset adalah individu yang bertanggungjawab untuk mengurus dan menyelenggara aset-aset sesebuah organisasi. Aset ini boleh merangkumi harta fizikal seperti bangunan, peralatan, kenderaan, serta aset digital seperti perisian, data, dan infrastruktur IT.
Pentadbir Sistem ICT	Terdiri daripada Pentadbir Sistem Aplikasi, Pentadbir Keselamatan, Pentadbir Rangkaian, Pentadbir Server, Pentadbir Laman Web, Pentadbir E-mel, Pentadbir Pangkalan Data, Pentadbir Aset dan Pentadbir Pusat Data.
Pentadbir Sistem Aplikasi	Pegawai yang menguruskan aplikasi atau perisian tertentu dalam jabatan. Bertanggungjawab memasang, mengemas kini dan menyelenggara aplikasi yang diberikan
Pentadbir Keselamatan	Pegawai yang bertanggungjawab untuk pentadbiran sistem keselamatan siber di sesebuah jabatan.
Pentadbir Rangkaian	Pegawai yang mengurus rangkaian dan bertanggungjawab untuk memasang, memantau aktiviti rangkaian, menyelesaikan masalah dan menaik taraf infrastruktur rangkaian, termasuk komponen peralatan dan perisian rangkaian.
Pentadbir Server	Pegawai teknikal yang mengawasi pelayan komputer
Pentadbir Laman Web	Pegawai teknikal yang menyelenggara laman web.
Pentadbir E-mel	Pegawai yang mengurus perkhidmatan e-mel.

ISTILAH	TAKRIF
Pentadbir Pangkalan Data	Pegawai yang mengurus, menyandarkan dan memastikan ketersediaan data yang dihasilkan dan digunakan oleh jabatan melalui sistem ICT.
Pentadbir Pengkomputeran Awan	Pentadbir Pengkomputeran Awan adalah individu yang bertanggungjawab untuk menguruskan dan menyelenggara perkhidmatan dan infrastruktur pengkomputeran awan bagi sesebuah organisasi. Memastikan bahawa perkhidmatan pengkomputeran awan berjalan dengan lancar, selamat, dan efisien.
Pentadbir Aset	Pegawai yang dilantik untuk mengurus penyelenggaraan aset.
Pentadbir Pusat Data	Pegawai yang bertanggungjawab untuk mengawasi operasi pusat data.
Penyelaras ICT Fasiliti	Pegawai ICT yang dilantik untuk bertanggungjawab mengurus dan menyelaras infrastruktur ICT fasiliti.
Peralatan ICT	Merangkumi semua jenis peralatan dan kelengkapan ICT seperti yang disenaraikan di dalam Sistem Pengurusan Aset Alih (SPA).
Peranti Peribadi	Peranti hak milik peribadi seperti (tidak terhad kepada) telefon, tablet, komputer, pencetak dan lain-lain peralatan ICT yang dibawa, digunakan dan disambungkan ke rangkaian komputer fasiliti
Peranti Titik Akhir	Merujuk kepada mana-mana peranti yang disambungkan dengan rangkaian komputer fasiliti.
Perisian ICT	Merangkumi semua jenis perisian sistem, perisian aplikasi dan lesen perisian (pembelian dan pembaharuan). Perisian sistem merangkumi sistem operasi, pangkalan data dan perisian bagi membangunkan sistem. Perisian aplikasi ialah perisian yang digunakan untuk menyokong kerja-kerja harian dalam urusan dan pentadbiran pejabat serta pengajaran dan pembelajaran.
Pesanan Elektronik	Mel elektronik dan sistem pemesejan elektronik lain yang digunakan untuk tujuan berkomunikasi antara individu. Komunikasi elektronik boleh dikelaskan seperti pemesejan, panggilan suara, e-mel, media sosial dan lain-lain.
Pihak ketiga	Pihak yang memberi perkhidmatan ICT merangkumi kontraktor, pembekal dan perunding.
PII	*Personally identifiable information (PII)* - Maklumat pengenalan peribadi Sebarang maklumat yang disambungkan kepada individu tertentu yang boleh digunakan untuk mendedahkan atau mencuri identiti individu tersebut, seperti nama penuh, alamat e-mel atau nombor telefon mereka
PKS	Polisi Keselamatan Siber (PKS) KKM merupakan dokumen dasar rasmi keselamatan siber KKM yang menetapkan peranan, tanggungjawab dan kawalan untuk melindungi aset maklumat KKM meliputi tadbir urus, pengurusan risiko, pemantauan/pematuhan dan penambahbaikan berterusan.
Router	Peralatan rangkaian yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan.
Sandaran	Proses menyalin data atau sistem komputer ke lokasi atau media simpanan lain dengan tujuan untuk pemulihan (recovery) sekiranya data asal hilang, rosak, atau tidak dapat diakses

ISTILAH	TAKRIF
SLA	*Service Level Agreement (SLA)* - Perjanjian peringkat perkhidmatan Perjanjian antara penyedia perkhidmatan dan pelanggan. Aspek tertentu perkhidmatan – kualiti, ketersediaan, tanggungjawab – dipersetujui antara penyedia perkhidmatan dan pengguna perkhidmatan. Komponen yang paling biasa dalam SLA ialah perkhidmatan perlu diberikan kepada pelanggan seperti yang dipersetujui dalam kontrak.
Pelayan	Merujuk kepada sistem komputer (atau program komputer) yang menyediakan sumber, data, perkhidmatan, atau program kepada komputer lain, yang dikenali sebagai "klien," melalui rangkaian..
Switches	Peranti rangkaian yang berfungsi untuk menghubungkan beberapa peranti dalam satu rangkaian tempatan *(LAN)* dan menghantar data secara langsung kepada peranti yang dituju berdasarkan alamat *MAC (Media Access Control)*
UPS	*Uninterruptible Power Supply (UPS)* Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Virus	Merujuk kepada perisian komputer berniat jahat (malicious software) yang direka untuk menjangkiti sistem komputer dan merebak ke fail atau komputer lain.




SURIANI

PRAKATA



Assalamualaikum Warahmatullahi Wabarakatuh dan Salam Sejahtera

Dalam era digital yang semakin berasaskan teknologi, keselamatan siber bukan lagi satu pilihan tetapi menjadi keperluan utama dalam menjamin kelangsungan dan ketahanan perkhidmatan jagaan kesihatan negara. Kementerian Kesihatan Malaysia (KKM) berhadapan dengan pelbagai ancaman dan cabaran dalam melindungi maklumat serta aset digital yang menjadi teras utama kepada operasi dan penyampaian perkhidmatan jagaan kesihatan kepada rakyat.

Polisi Keselamatan Siber (PKS) KKM digubal sebagai panduan menyeluruh bagi memperkukuh tadbir urus, pengurusan risiko dan kawalan keselamatan siber di seluruh struktur organinasi dalam kementerian ini. Polisi ini menegaskan tanggungjawab bersama seluruh warga KKM dan pihak berkepentingan untuk memastikan maklumat kerajaan sentiasa terpelihara daripada sebarang ancaman, pencerobohan serta penyalahgunaan.

Pelaksanaan PKS ini mencerminkan komitmen berterusan KKM dalam membudayakan amalan keselamatan siber yang berteraskan prinsip akauntabiliti, integriti dan ketersediaan sepanjang masa. Saya menyeru semua pihak agar memberikan kerjasama padu dan komitmen sepenuhnya dalam melaksanakan polisi ini, selaras dengan hala tuju KKM ke arah memperkukuh ekosistem kesihatan digital yang mampan, berdaya tahan dan selamat demi kesejahteraan rakyat.

Sekian, terima kasih.

Dato' Sri Suriani binti Dato' Ahmad
Ketua Setiausaha
Kementerian Kesihatan Malaysia

ISI KANDUNGAN

1.0 PENGENALAN

1.1 LATAR BELAKANG 3
1.2 TUJUAN 3
1.3 OBJEKTIF 4
1.4 KEPIMPINAN & KOMITMEN 4

2.0 SKOP & PIHAK BERKEPENTINGAN

2.1 SKOP POLISI 7
2.2 PIHAK BERKEPENTINGAN 8

3.0 TADBIR URUS KESELAMATAN MAKLUMAT

3.1 PRINSIP-PRINSIP KESELAMATAN MAKLUMAT 11
3.2 PERANAN & TANGGUNGJAWAB 12
3.3 SUMBER, KOMPETENSI & KESEDARAN 13
3.4 KOMUNIKASI 14
3.5 DOKUMENTASI 14

4.0 PENGURUSAN RISIKO KESELAMATAN MAKLUMAT

4.1 PENILAIAN RISIKO 17
4.2 KAWALAN RISIKO & PELAKSANAAN 17
4.3 PEMANTAUAN, AUDIT & SEMAKAN 17
4.4 PENAMBAHBAIKAN BERTERUSAN 18

5.0 BAB ORGANISASI

5.1 POLISI KESELAMATAN MAKLUMAT 21
(POLICIES FOR INFORMATION SECURITY)
5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT 22
(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)
5.3 PENGASINGAN TUGAS 29
(SEGREGATION OF DUTIES)
5.4 TUGAS DAN TANGGUNGJAWAB PENGURUSAN 30
(MANAGEMENT RESPONSIBILITIES)
5.5 HUBUNGAN DENGAN PIHAK BERKUASA 31
(CONTACT WITH AUTHORITIES)
5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN 31
(CONTACT WITH SPECIAL INTEREST GROUPS)
5.7 PERISIKAN ANCAMAN 32
(THREAT INTELLIGENCE)

5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK 33
(INFORMATION SECURITY IN PROJECT MANAGEMENT)
5.9 INVENTORI MAKLUMAT DAN ASET BERKAITAN YANG LAIN 34
(INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS)
5.10 PENGGUNAAN YANG DITERIMA BAGI MAKLUMAT DAN ASET BERKAITAN YANG LAIN 35
(ACCEPTABLE USE OF INFORMATION AND OTHER ASSOCIATED ASSETS)
5.11 PEMULANGAN ASET 35
(RETURN OF ASSETS)
5.12 PENGELASAN MAKLUMAT 36
(CLASSIFICATION OF INFORMATION)
5.13 PELABELAN MAKLUMAT 38
(LABELLING OF INFORMATION)
5.14 PEMINDAHAN MAKLUMAT 38
(INFORMATION TRANSFER)
5.15 KAWALAN CAPAIAN 42
(ACCESS CONTROL)
5.16 PENGURUSAN IDENTITI 43
(IDENTITY MANAGEMENT)
5.17 PENGESAHAN MAKLUMAT 44
(AUTHENTICATION INFORMATION)
5.18 HAK CAPAIAN 46
(ACCESS RIGHTS)
5.19 KESELAMATAN MAKLUMAT DALAM HUBUNGAN PIHAK KETIGA 48
(INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS)
5.20 MENANGANI KESELAMATAN MAKLUMAT DALAM PERJANJIAN PIHAK KETIGA 49
(ADDRESSING INFORMATION SECURITY WITHIN SUPPLIER AGREEMENTS)
5.21 MENGURUS KESELAMATAN MAKLUMAT DALAM RANTAIAN BEKALAN ICT 50
(MANAGING INFORMATION SECURITY IN THE ICT SUPPLY CHAIN)
5.22 PEMANTAUAN , PENILAIAN DAN PENGURUSAN PERUBAHAN PERKHIDMATAN PIHAK KETIGA 51
(MONITORING, REVIEW AND CHANGE MANAGEMENT OF SUPPLIER SERVICES)
5.23 KESELAMATAN MAKLUMAT UNTUK PENGGUNAAN PERKHIDMATAN AWAN 52
(INFORMATION SECURITY FOR USE OF CLOUD SERVICES)
5.24 PERANCANGAN DAN PENYEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT 54
(INFORMATION SECURITY INCIDENT MANAGEMENT PLANNING AND PREPARATION)
5.25 PENILAIAN DAN KEPUTUSAN MENGENAI INSIDEN KESELAMATAN MAKLUMAT 55
(ASSESSMENT AND DECISION ON INFORMATION SECURITY EVENTS)
5.26 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT 56
(RESPONSE TO INFORMATION SECURITY INCIDENTS)

5.27 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT 56
(LEARNING FROM INFORMATION SECURITY INCIDENTS)
5.28 PENGUMPULAN BUKTI 57
(COLLECTION OF EVIDENCE)
5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN 57
(INFORMATION SECURITY DURING DISRUPTION)
5.30 KESEDIAAN ICT UNTUK KESINAMBUNGAN PERKHIDMATAN 58
(ICT READINESS FOR BUSINESS CONTINUITY)
5.31 UNDANG-UNDANG, BERKANUN, PERATURAN DAN KEPERLUAN KONTRAK 60
(LEGAL, STATUTORY, REGULATORY AND CONTRACTUAL REQUIREMENTS)
5.32 HAK HARTA INTELEK 61
(INTELLECTUAL PROPERTY RIGHTS)
5.33 PERLINDUNGAN REKOD 61
(PROTECTION OF RECORDS)
5.34 PRIVASI DAN PERLINDUNGAN DATA PERIBADI 62
(PRIVACY AND PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION)
5.35 KAJIAN SEMULA KESELAMATAN MAKLUMAT SECARA BERKECUALI 62
(INDEPENDENT REVIEW OF INFORMATION SECURITY)
5.36 KEPATUHAN TERHADAP DASAR, PERATURAN, DAN STANDARD KESELAMATAN MAKLUMAT 63
(COMPLIANCE WITH POLICIES, RULES AND STANDARDS FOR INFORMATION SECURITY)
5.37 DOKUMENTASI PROSEDUR 63
(DOCUMENTED OPERATING PROCEDURES)

6.0 BAB MANUSIA

6.1 TAPISAN KESELAMATAN 67
(SCREENING)
6.2 SYARAT-SYARAT PEKERJAAN 67
(TERMS AND CONDITIONS OF EMPLOYMENT)
6.3 PROGRAM KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT 67
(INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING)
6.4 PROSES TATATERTIB 68
(DISCIPLINARY PROCESS)
6.5 TANGGUNGJAWAB SELEPAS PENAMATAN ATAU PERTUKARAN PERKHIDMATAN 68
(RESPONSIBILITIES AFTER TERMINATION OR CHANGE OF EMPLOYMENT)
6.6 PERJANJIAN KERAHSIAAN DAN KETIDAKDEDAHAN 70
(CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS)
6.7 BEKERJA SECARA JARAK JAUH 70
(REMOTE WORKING)

6.8 PELAPORAN PERISTIWA KESELAMATAN MAKLUMAT 70
(INFORMATION SECURITY EVENT REPORTING)

7.0 BAB FIZIKAL

7.1 PERIMETER KESELAMATAN FIZIKAL 75
(PHYSICAL SECURITY PERIMETERS)
7.2 KEMASUKAN FIZIKAL 75
(PHYSICAL ENTRY)
7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN 76
(SECURING OFFICES, ROOMS AND FACILITIES)
7.4 PEMANTAUAN KESELAMATAN FIZIKAL 77
(PHYSICAL SECURITY MONITORING)
7.5 PERLINDUNGAN DARIPADA ANCAMAN FIZIKAL DAN ALAM SEKITAR 78
(PROTECTING AGAINST PHYSICAL AND ENVIRONMENTAL THREATS)
7.6 BEKERJA DI KAWASAN TERKAWAL 78
(WORKING IN SECURE AREAS)
7.7 POLISI MEJA SELAMAT DAN PAPARAN SELAMAT 79
(CLEAR DESK AND CLEAR SCREEN)
7.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN 79
(EQUIPMENT SITING AND PROTECTION)
7.9 KESELAMATAN ASET DI LUAR PREMIS 81
(SECURITY OF ASSETS OFF-PREMISES)
7.10 PENYIMPANAN MEDIA 81
(STORAGE MEDIA)
7.11 UTILITI SOKONGAN 83
(SUPPORTING UTILITIES)
7.12 KESELAMATAN KABEL 83
(CABLING SECURITY)
7.13 PENYELENGGARAAN PERALATAN 84
(EQUIPMENT MAINTENANCE)
7.14 PELUPUSAN ATAU PENGGUNAAN SEMULA PERALATAN DENGAN SELAMAT 85
(SECURE DISPOSAL OR RE-USE OF EQUIPMENT)

8.0 BAB TEKNOLOGI

8.1 PERANTI TITIK AKHIR PENGGUNA 89
(USER ENDPOINT DEVICES)
8.2 HAK CAPAIAN ISTIMEWA 90
(PRIVILEGED ACCESS RIGHTS)
8.3 SEKATAN CAPAIAN MAKLUMAT 91
(INFORMATION ACCESS RESTRICTION)

8.4 CAPAIAN KEPADA KOD SUMBER 93
(ACCESS TO SOURCE CODE)
8.5 PENGESAHAN SELAMAT 93
(SECURE AUTHENTICATION)
8.6 PENGURUSAN KAPASITI 95
(CAPACITY MANAGEMENT)
8.7 PERLINDUNGAN TERHADAP PERISIAN HASAD 96
(PROTECTION AGAINST MALWARE)
8.8 PENGURUSAN KERENTANAN TEKNIKAL 97
(MANAGEMENT OF TECHNICAL VULNERABILITIES)
8.9 PENGURUSAN KONFIGURASI 99
(CONFIGURATION MANAGEMENT)
8.10 PENGHAPUSAN MAKLUMAT 100
(INFORMATION DELETION)
8.11 PENYAMARAN DATA 100
(DATA MASKING)
8.12 PENCEGAHAN KEBOCORAN DATA 101
(DATA LEAKAGE PREVENTION)
8.13 SANDARAN MAKLUMAT 102
(INFORMATION BACKUP)
8.14 LEWAHAN FASILITI PEMPROSESAN MAKLUMAT 102
(REDUNDANCY OF INFORMATION PROCESSING FACILITIES)
8.15 LOG 104
(LOGGING)
8.16 AKTIVITI PEMANTAUAN 105
(MONITORING ACTIVITIES)
8.17 PENYELARASAN WAKTU 106
(CLOCK SYNCHRONIZATION)
8.18 PENGGUNAAN PROGRAM UTILITI ISTIMEW 106
(USE OF PRIVILEGED UTILITY PROGRAMS)
8.19 PEMASANGAN PERISIAN PADA SISTEM OPERASI 107
(INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS)
8.20 KESELAMATAN RANGKAIAN 108
(NETWORK SECURITY)
8.21 KESELAMATAN PERKHIDMATAN RANGKAIAN 110
(SECURITY OF NETWORK SERVICES)
8.22 PENGASINGAN RANGKAIAN 110
(SEGREGATION OF NETWORKS)
8.23 PENAPISAN WEB 111
WEB FILTERING)

8.24 PENGGUNAAN KRIPTOGRAFI 112
(USE OF CRYPTOGRAPHY)
8.25 KITARAN HAYAT PEMBANGUNAN SELAMAT 116
(SECURE DEVELOPMENT LIFE CYCLE)
8.26 KEPERLUAN KESELAMATAN APLIKASI 116
(APPLICATION SECURITY REQUIREMENTS)
8.27 PRINSIP SENI BINA DAN KEJURUTERAAN SISTEM YANG SELAMAT 118
(SECURE SYSTEM ARCHITECTURE AND ENGINEERING PRINCIPLES)
8.28 PENGEKODAN SELAMAT 120
(SECURE CODING)
8.29 UJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN 121
(SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE)
8.30 PEMBANGUNAN SUMBER LUAR 123
(OUTSOURCED DEVELOPMENT)
8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PRODUKSI 124
(SEPARATION OF DEVELOPMENT, TEST AND PRODUCTION ENVIRONMENTS)
8.32 PENGURUSAN PERUBAHAN 126
(CHANGE MANAGEMENT)
8.33 MAKLUMAT PENGUJIAN 127
(TEST INFORMATION)
8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PENGUJIAN AUDIT 127
(PROTECTION OF INFORMATION SYSTEMS DURING AUDIT TESTING)

LAMPIRAN

SURAT AKUAN PEMATUHAN 131
PERAKUAN AKTA RAHSIA RASMI 1972 [AKTA 88] 132
PERJANJIAN KERAHSIAAN 133
PERJANJIAN UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI 134

SIDANG REDAKSI

SIDANG REDAKSI 137



1.0

PENGENALAN





1.1 LATAR BELAKANG

Dokumen ini merupakan panduan utama bagi pegawai serta pihak-pihak yang terlibat dalam pengurusan data atau maklumat di Kementerian Kesihatan Malaysia (KKM). Polisi Keselamatan Siber (PKS) KKM memperincikan peranan, tanggungjawab, arahan, peraturan, garis panduan, dan amalan yang **MESTI DIBACA DAN DIPATUHI** oleh pegawai KKM dan pihak ketiga yang memberikan perkhidmatan teknologi maklumat di KKM dalam melindungi aset dan maklumat daripada capaian yang tidak sah, kehilangan atau kebocoran yang membawa kesan yang memudaratkan kepada penyampaian perkhidmatan jagaan kesihatan di Malaysia.



1.2 TUJUAN

Tujuan polisi ini dibangunkan adalah untuk dijadikan satu rangka kerja yang sistematik dalam menguruskan keselamatan siber, memberi panduan untuk penambahbaikan, kesiapsiagaan menghadapi ancaman, meningkatkan kepercayaan pihak berkepentingan serta memastikan pematuhan kepada arahan, garis panduan, akta dan undang-undang berkait keselamatan siber di Malaysia selaras dengan penambahbaikan Standard Antarabangsa iaitu Information Security Management System (ISMS) IISO/IEC 27001:2022



1.3 OBJEKTIF

PKS KKM dibangunkan untuk mencapai objektif utama berikut:

(a) melindungi pihak-pihak yang berkepentingan yang menggunakan sistem maklumat dari kesan kegagalan atau kelemahan dalam aspek kerahsiaan, integriti, kebolehsediaan dan kesahihan maklumat serta penyangkalan;

(b) mematuhi keperluan perundangan, peraturan, standard, pekeliling dan prosedur yang sedang berkuatkuasa;

(c) memastikan penyampaian perkhidmatan di KKM pada tahap keselamatan tertinggi yang dapat meningkatkan keyakinan pihak berkepentingan seperti jabatan kerajaan, industri dan orang awam;

(d) menjamin kelancaran operasi dan kesinambungan perkhidmatan KKM dengan meminimumkan impak insiden keselamatan siber;

(e) mencegah sebarang penyalahgunaan atau kecurian maklumat kerajaan;

(f) menyediakan asas bagi penambahbaikan yang berterusan dalam pengurusan keselamatan dan pentadbiran teknologi maklumat (ICT);

(g) Memudahkan perkongsian maklumat yang selamat dan terjamin.

1.4 KEPIMPINAN & KOMITMEN

01 KEPIMPINAN

- Menetapkan **hala tuju** keselamatan siber yang jelas.
- Menjadi **contoh teladan** dalam pematuhan polisi.
- Memastikan **akauntabiliti** wujud di semua peringkat pengurusan.

02 KOMITMEN

- Memastikan **sumber kewangan dan tenaga kerja** mencukupi.
- Menyokong **program kesedaran dan latihan** keselamatan siber.
- Menubuhkan **Jawatankuasa Pemandu** Keselamatan Siber.

03 PELAKSANAAN

- Memastikan PKS **difahami dan dipatuhi** di semua peringkat.
- Mengintegrasikan keselamatan siber dalam **semua proses kerja**.
- Memantau dan **menyemak semula polisi** secara berkala.



2.0



SKOP & PIHAK BERKEPENTINGAN

2.1 SKOP POLISI

Polisi Keselamatan Siber KKM ini merangkumi perlindungan semua bentuk maklumat Kerajaan yang dimasukkan, diwujudkan, dihapuskan, disimpan, dijana, dicetak, dicapai, diedarkan, dalam penghantaran dan yang dibuat salinan keselamatan bagi menentukan aset ini terjamin keselamatannya sepanjang masa. Ini dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur pengendalian semua perkara-perkara berikut:

(a) **Perkakasan**

Diguna untuk menyokong pemprosesan dan penyimpanan maklumat.

(Contohnya: Komputer meja, komputer riba, pelayan atau pencetak);

(b) **Perisian**

Perisian aplikasi atau sistem yang menyediakan kemudahan pemprosesan maklumat.

(Contohnya: Perisian sistem operasi, Perisian pakej/standard, Aplikasi perkhidmatan);

(c) **Perkhidmatan**

Perkhidmatan sokongan dan perkhidmatan capaian yang menyokong aset lain untuk melaksana fungsinya.

(Contohnya: Penghawa dingin, Bekalan elektrik, *Fire Suppression System*, LAN, WAN, VPN, WiFi);

(d) **Proses Kerja**

Proses kerja utama dan sokongan.

(Contohnya: Proses pembayaran gaji, Proses pelesenan pihak ketiga, atau Proses pendaftaran pelajar.)

(e) **Maklumat**

Mengandungi data (salinan digital atau salinan cetak) yang telah diproses, disusun dan mempunyai makna kepada penerima. dan mempunyai makna kepada penerima.

(Contohnya: Data pelajar, Laporan gaji, Profil pelanggan);

(f) **Sumber Manusia**

Individu yang terlibat dalam proses kerja atau / dan pemprosesan maklumat

(Contohnya: Ketua Penolong Setiausaha, Penolong Setiausaha atau Juruteknik);

(g) **Premis**

Premis yang diguna untuk menempatkan perkara (a) – (g)

(Contohnya: Bangunan pejabat)

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai pelanggaran langkah-langkah kawalan keselamatan.

2.2 PIHAK BERKEPENTINGAN

Pihak berkepentingan adalah individu, kumpulan atau organisasi yang mempunyai kepentingan langsung atau tidak langsung terhadap keselamatan siber di KKM. Mengenal pasti pihak berkepentingan adalah penting untuk memastikan keperluan, jangkaan dan tanggungjawab mereka diambil kira dalam pelaksanaan dan pengurusan polisi ini.

Senarai kategori pihak berkepentingan:

(a) Pengurusan Tertinggi KKM – menetapkan hala tuju strategik, meluluskan dasar serta menyediakan sumber berkaitan keselamatan siber.

(b) Pegawai & Kakitangan KKM – melaksanakan tugas mengikut prosedur keselamatan siber yang ditetapkan.

(c) Bahagian/Unit Teknologi Maklumat – bertanggungjawab menyelaras dan memantau kawalan teknikal dan pentadbiran keselamatan siber.

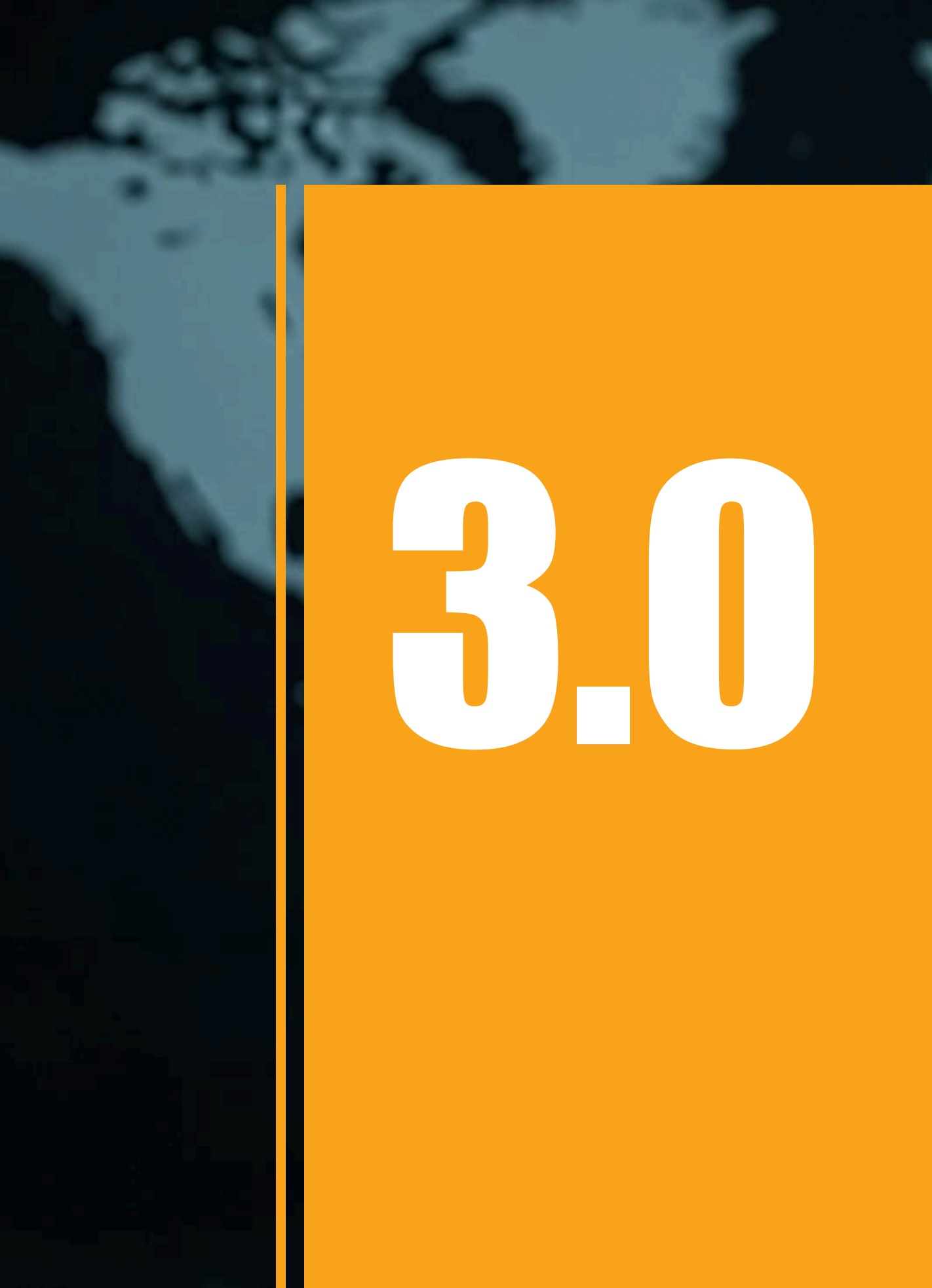
(d) Pelanggan & Orang Awam – bergantung kepada perkhidmatan KKM yang memerlukan perlindungan data peribadi dan maklumat kesihatan.

(e) Rakan Strategik & Pembekal – termasuk kontraktor ICT, penyedia perkhidmatan awan, dan vendor teknologi yang terlibat dalam pembangunan, operasi atau penyelenggaraan sistem KKM.

(f) Agensi Pengawal Selia / Kerajaan Pusat – seperti (tidak terhad kepada) JDN, CGSO dan NACSA, yang menetapkan dasar, piawaian dan pematuhan keselamatan siber.

(g) Pihak Audit Dalaman & Luaran – memastikan keberkesanan pelaksanaan PKS dan pematuhan terhadap piawaian.





3.0



TADBIR URUS KESELAMATAN MAKLUMAT

3.1 PRINSIP-PRINSIP KESELAMATAN MAKLUMAT

KKM mengguna pakai prinsip asas keselamatan maklumat sebagai panduan utama dalam pengurusan aset maklumat dan sistem ICT, bagi memastikan kerahsiaan, integriti, ketersediaan, kesahihan dan pematuhan sentiasa terjamin selaras dengan undang-undang dan dasar kerajaan yang berkuat kuasa.

(a) Capaian Atas Dasar Perlu Mengetahui

Akses kepada aset hanya diberikan untuk tujuan yang sah dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui". Pertimbangan capaian dibuat berdasarkan pengelasan dan peringkat dokumen seperti yang dinyatakan dalam Arahan Keselamatan Kerajaan.

(b) Hak Capaian Minimum

Pengguna hendaklah diberikan hak capaian minimum iaitu hanya setakat yang diperlukan untuk melaksanakan tugas. Kelulusan khas diperlukan untuk mewujud, menyimpan, mengemas kini, mengubah atau menghapus maklumat.

(c) Akauntabiliti

Semua pengguna bertanggungjawab atas tindakan mereka terhadap aset ICT KKM. Sistem ICT perlu menyokong fungsi pengesanan (audit trail) untuk memastikan setiap tindakan boleh dikenal pasti. Akauntabiliti merangkumi pencegahan pendedahan tidak sah, ketepatan maklumat, pematuhan prosedur, kerahsiaan kata laluan, serta pemeliharaan kawalan keselamatan sepanjang kitaran hayat maklumat.

(d) Pengasingan Tugas

Tugas kritikal hendaklah diasingkan untuk mengelakkan capaian tidak dibenarkan, kesilapan atau manipulasi data. Peranan seperti mewujud, mengemaskini, meluluskan dan mengesahkan data perlu diagihkan kepada pegawai berbeza bagi mengekalkan prinsip check and balance.

(e) Prinsip Kepercayaan Sifar *(Zero Trust)*

Tiada pengguna, peranti atau rangkaian dipercayai secara automatik sama ada dari dalam atau luar organisasi. Semua akses perlu melalui pengesahan identiti, status peranti dan faktor konteks lain. Capaian hanya dibenarkan mengikut prinsip hak capaian minimum, apabila perlu, dan untuk tempoh yang terhad.

(f) Pengauditan

Aktiviti berkaitan keselamatan ICT hendaklah direkod dan dianalisis bagi memastikan pematuhan. Aset ICT seperti pelayan, firewall dan peralatan rangkaian perlu berupaya menjana serta menyimpan log keselamatan untuk tujuan audit.

(g) Pematuhan

Semua pegawai, kakitangan dan pihak ketiga wajib membaca, memahami dan mematuhi PKS ini. Pelanggaran dianggap ancaman kepada keselamatan siber dan boleh dikenakan tindakan.

(h) Pemulihan

Pelan pemulihan bencana dan kesinambungan perkhidmatan hendaklah diwujudkan untuk memastikan maklumat kekal tersedia dan meminimumkan gangguan operasi.

(i) Saling Bergantungan

Prinsip-prinsip keselamatan saling melengkapi antara satu sama lain dan perlu dilaksanakan secara bersepadu untuk menghasilkan perlindungan menyeluruh.

(j) Ciri-Ciri Keselamatan Data dan Maklumat

i. Kerahsiaan – melindungi maklumat daripada capaian tidak dibenarkan.

ii. Integriti – memastikan maklumat tepat, lengkap dan tidak diubah tanpa kebenaran.

iii. Tidak Boleh Disangkal – menjamin pihak yang terlibat dalam transaksi tidak boleh menafikan penglibatan mereka.

iv. Kesahihan – memastikan maklumat sah dan berasal daripada sumber yang dipercayai.

v. Ketersediaan – memastikan maklumat boleh dicapai bila diperlukan oleh pihak yang diberi kuasa.

3.2 PERANAN & TANGGUNGJAWAB

Setiap individu dalam KKM bertanggungjawab menjaga keselamatan maklumat mengikut peranan dan fungsi masing-masing. Pengurusan atasan hendaklah menunjukkan kepimpinan dan menyediakan hala tuju manakala penyelaras dan pentadbir keselamatan maklumat di peringkat kementerian, jabatan dan bahagian bertanggungjawab menyelaras pelaksanaan kawalan keselamatan maklumat, memantau keberkesanan kawalan teknikal dan pentadbiran, serta melaporkan status keselamatan ICT kepada Jawatankuasa Pemandu ICT (JPICT).

Ketidakpatuhan terhadap PKS boleh mengakibatkan implikasi serius termasuk tetapi tidak terhad kepada:

(a) Gangguan Operasi: Ketidakpatuhan boleh menyebabkan gangguan kepada operasi harian KKM, termasuk masa henti sistem, kehilangan data, dan kerosakan peralatan, yang boleh memberi kesan langsung kepada penyampaian perkhidmatan.

(b) Kesan Undang-Undang: Kegagalan mematuhi polisi ini boleh menyebabkan tindakan undang-undang diambil terhadap pihak yang terlibat, termasuk denda atau tindakan undang-undang lain yang berkaitan dengan pelanggaran peraturan dan undang-undang keselamatan siber.

(c) Kerugian Kewangan: Ketidakpatuhan boleh membawa kepada kerugian kewangan yang besar, sama ada melalui denda, kos pemulihan, atau kehilangan kepercayaan pelanggan dan pihak berkepentingan yang boleh menjejaskan kedudukan kewangan KKM.

(d) Kerosakan Reputasi: Insiden keselamatan siber yang disebabkan oleh ketidakpatuhan boleh merosakkan reputasi, mengurangkan kepercayaan pihak berkepentingan dan masyarakat umum terhadap keupayaan KKM dalam penyampaian perkhidmatan jagaan kesihatan.

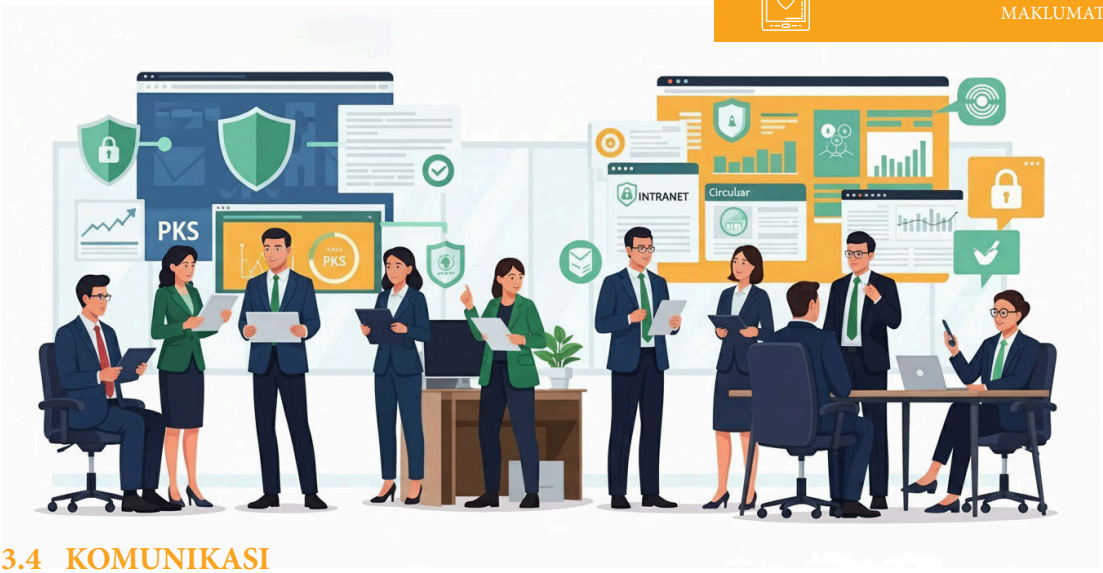
(e) Tindakan Disiplin: Pegawai yang didapati tidak mematuhi PKS ini boleh dikenakan tindakan disiplin, termasuk amaran, penggantungan, atau penamatan perkhidmatan, bergantung kepada tahap pelanggaran yang dilakukan.

3.3 SUMBER, KOMPETENSI & KESEDARAN

Penggunaan sumber manusia, kewangan dan teknologi yang ada perlu dioptimumkan bagi memastikan pelaksanaan PKS dapat dijalankan secara berkesan. Pegawai yang terlibat hendaklah dikenal pasti dan dibekalkan dengan kompetensi yang bersesuaian mengikut peranan masing-masing.

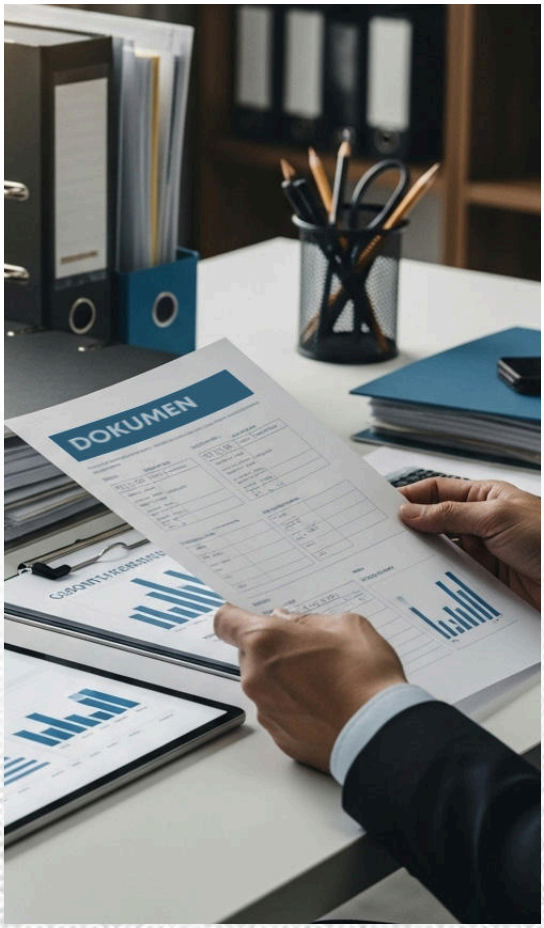
Bagi meningkatkan tahap pemahaman serta kesiapsiagaan, program latihan dan kesedaran keselamatan maklumat perlu dilaksanakan secara berterusan. Usaha ini bertujuan membentuk budaya keselamatan siber yang konsisten di semua peringkat organisasi dan mengurangkan risiko insiden keselamatan maklumat.





3.4 KOMUNIKASI

Komunikasi mengenai PKS hendaklah disampaikan secara jelas dan berkesan kepada semua pihak berkepentingan di KKM. Penyebaran maklumat boleh dilaksanakan melalui medium rasmi seperti portal intranet, pekeliling, garis panduan, latihan atau taklimat berkala. Komunikasi yang berkesan memastikan setiap individu memahami dan melaksanakan kawalan keselamatan maklumat dengan penuh tanggungjawab.

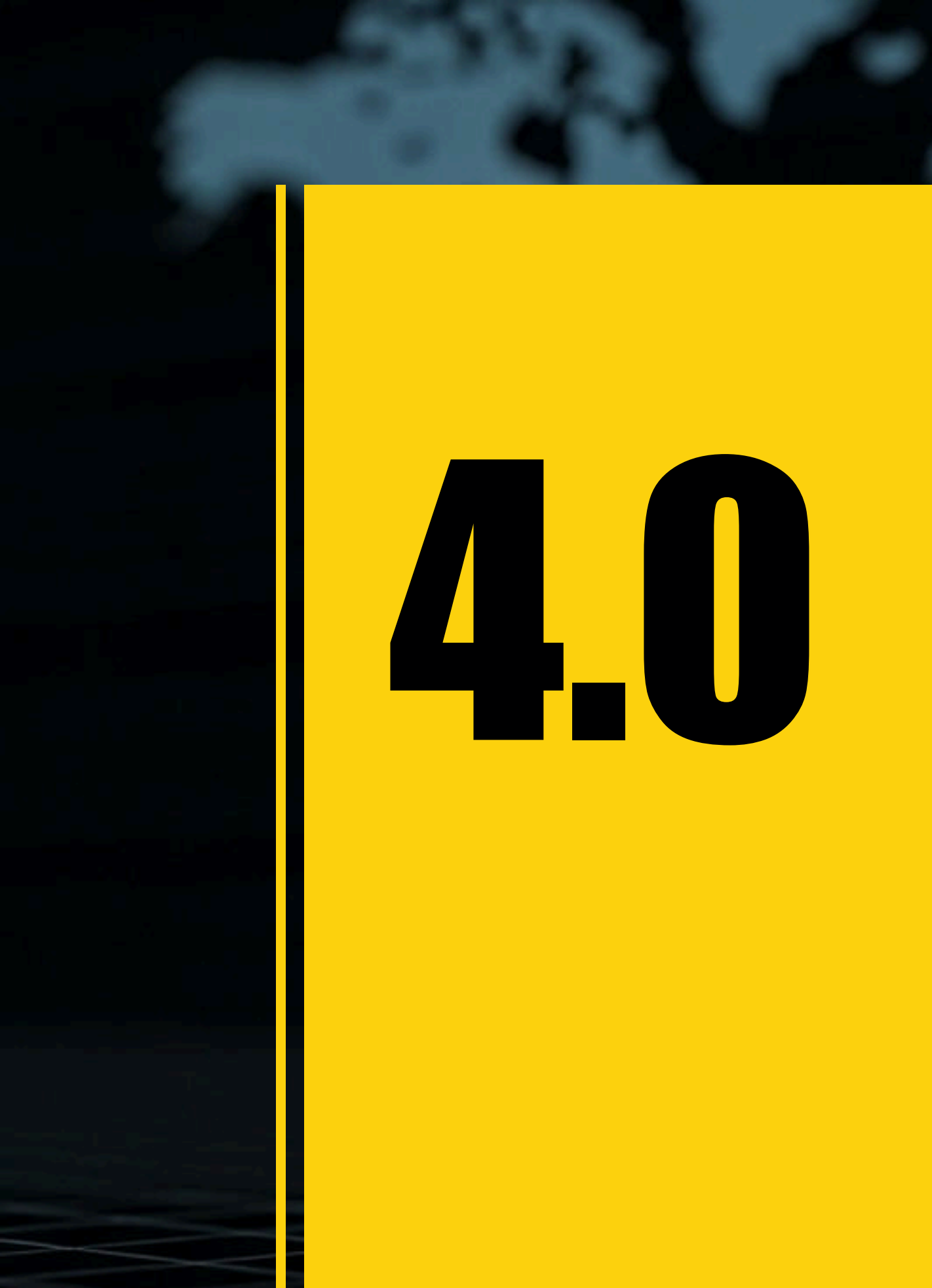




3.5 DOKUMENTASI

Semua dokumen yang berkaitan dengan PKS, termasuk dasar, prosedur, garis panduan, rekod dan laporan, hendaklah direkod, dikawal, disemak semula serta dikemas kini secara berkala mengikut keperluan KKM.

Pengurusan dokumentasi ini perlu dilaksanakan secara sistematik bagi memastikan dokumen sentiasa terkini, sah digunakan, boleh dipercayai, dan mudah diakses oleh pihak yang diberi kuasa. Kaedah pengurusan hendaklah mengambil kira dasar serta peraturan kerajaan yang berkuat kuasa, di samping amalan terbaik dalam keselamatan maklumat.


4.0



PENGURUSAN RISIKO KESELAMATAN MAKLUMAT

4.1 PENILAIAN RISIKO

Seiring dengan perkembangan perkhidmatan pendigitalan, sistem penyampaian perkhidmatan KKM semakin terdedah kepada pelbagai risiko serangan siber seperti penafian perkhidmatan, pencerobohan dan jangkitan perisian hasad. Bagi memastikan perkhidmatan KKM sentiasa berada pada tahap terbaik serta maklumat KKM kekal tersedia dan berintegriti, risiko keselamatan maklumat perlu dikenal pasti dan ditangani secara berkesan.

Pengurusan risiko keselamatan maklumat dilaksanakan melalui proses penilaian risiko yang merangkumi langkah-langkah berikut:

(a) mengenal pasti risiko yang berpotensi menjejaskan aset maklumat;

(b) menganalisis risiko dengan mengambil kira kebarangkalian dan impaknya;

(c) menilai tahap risiko berdasarkan kriteria penerimaan risiko yang ditetapkan; dan

(d) menetapkan kawalan atau tindakan mitigasi yang bersesuaian.

Penilaian risiko hendaklah dilaksanakan secara berkala dan berpandukan kawalan, akta, dasar serta pekeliling kerajaan yang sedang berkuat kuasa.

4.2 KAWALAN RISIKO & PELAKSANAAN

Kawalan keselamatan maklumat hendaklah dilaksanakan berdasarkan hasil penilaian risiko yang dijalankan. Kawalan ini bertujuan mengurangkan tahap risiko ke paras yang boleh diterima oleh organisasi, serta memastikan kesinambungan perkhidmatan dan perlindungan aset maklumat kerajaan.

Kawalan yang dilaksanakan merangkumi aspek berikut:

a. Teknikal – contohnya kawalan capaian, penyulitan, pemantauan rangkaian, sistem pengesanan pencerobohan dan perlindungan peranti.

b. Pentadbiran – termasuk dasar, prosedur, pengurusan identiti, pemantauan pematuhan, serta penguatkuasaan peraturan keselamatan.

c. Fizikal – seperti kawalan ke atas fasiliti, sistem sokongan, peralatan, dan persekitaran kerja untuk melindungi aset maklumat daripada ancaman atau kerosakan.

d. Prosedur Operasi – melibatkan langkah kerja, garis panduan dan pelan tindak balas insiden yang jelas serta dilaksanakan secara konsisten.

Pemilihan dan pelaksanaan kawalan hendaklah mengambil kira keperluan operasi, dasar kerajaan, peraturan keselamatan yang berkuat kuasa, serta amalan terbaik keselamatan maklumat.

4.3 PEMANTAUAN, AUDIT & SEMAKAN

Prestasi kawalan keselamatan maklumat yang dilaksanakan hendaklah dipantau secara berterusan bagi memastikan keberkesanan dan kesesuaiannya. Pemantauan ini merangkumi pengesanan insiden, semakan log keselamatan, serta penilaian tahap pematuhan terhadap dasar dan prosedur yang ditetapkan.

Audit dalaman keselamatan maklumat perlu dijalankan secara berkala bagi menilai sama ada kawalan keselamatan telah dilaksanakan dengan berkesan dan mematuhi keperluan KKM serta peraturan yang berkuat kuasa. Hasil audit hendaklah direkod dan dilaporkan kepada

pengurusan untuk tindakan pembetulan.

Selain itu, semakan pengurusan perlu dilaksanakan bagi menilai prestasi keseluruhan PKS, mengenal pasti jurang atau kelemahan, serta menentukan keperluan penambahbaikan. Semakan ini hendaklah dijalankan sebagaimana yang telah ditetapkan oleh KKM, termasuk apabila berlaku perubahan ketara terhadap persekitaran teknologi dan ancaman keselamatan siber.

4.4 PENAMBAHBAIKAN BERTERUSAN



Penambahbaikan berterusan merupakan elemen penting dalam memastikan PKS sentiasa relevan dan berkesan. Kelemahan atau jurang yang dikenal pasti melalui pemantauan, audit, insiden keselamatan, atau semakan pengurusan hendaklah ditangani dengan segera melalui tindakan pembetulan dan pencegahan yang bersesuaian.

KKM akan memastikan PKS ditambah baik secara berterusan bagi menyesuaikan dengan perubahan teknologi, perkembangan perkhidmatan digital, serta landskap ancaman keselamatan siber yang sentiasa berubah. Langkah penambahbaikan ini juga bertujuan meningkatkan tahap kesiapsiagaan KKM dalam melindungi aset maklumat dan menjamin kelangsungan perkhidmatan kesihatan awam.


5.0

BAB
ORGANISASI



5.1 POLISI KESELAMATAN MAKLUMAT *(POLICIES FOR INFORMATION SECURITY)*	PERANAN
5.1.1 Pelaksanaan Polisi Satu set polisi untuk keselamatan siber perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan KKM kepada pengguna, pembekal, pakar runding dan pihak yang berkepentingan yang berkaitan.	KSU
5.1.2 Pengesahan Polisi JPICT atau tadbir urus yang bersesuaian mesti meluluskan polisi, yang mesti disemak secara berkala jika perubahan berlaku dalam persekitaran keselamatan maklumat.	JPICT KKM
5.1.3 Penguatkuasaan Polisi PKS KKM mestilah dipatuhi oleh semua pegawai KKM, pembekal, pakar runding dan pihak yang berkepentingan yang berkaitan. Kegagalan mematuhi polisi ini boleh dikenakan tindakan tatatertib atau undang-undang berdasarkan peraturan dan perundangan semasa yang berkuat kuasa.	Pegawai KKM Pihak ketiga
5.1.4 Penyebaran Polisi Program kesedaran tentang polisi ini hendaklah dilaksanakan dan diselaraskan.	ICTSO Penyelaras ICT Fasiliti
5.1.5 Pengecualian Polisi PKS ini terpakai kepada semua pihak yang terlibat dalam penggunaan perkhidmatan dan aset ICT KKM tanpa sebarang pengecualian diberikan.	Semua
5.1.6 Penyelenggaraan Polisi Polisi keselamatan maklumat perlu dikaji mengikut keperluan untuk memastikan kesesuaian, kecukupan dan keberkesanannya yang berterusan.	CDO JPICT ICTSO
5.1.7 Kajian Semula/Semakan Polisi Berikut adalah prosedur berhubung dengan perubahan atau kajian semula PKS KKM: (a) mengenal pasti dan menentukan perubahan yang diperlukan; (b) kemuka cadangan secara bertulis dan dibuat 5 tahun sekali (c) mengemukakan cadangan perubahan kepada CDO untuk pembentangan dan persetujuan JPICT atau tadbir urus yang bersesuaian; dan (d) memaklumkan perubahan polisi yang telah dipersetujui oleh JPICT atau tadbir urus yang bersesuaian kepada semua pegawai KKM, pihak ketiga dan pihak yang mempunyai urusan perkhidmatan ICT dengan KKM (d) merekod dan menyimpan semua versi perubahan dalam log semakan polisi secara berpusat bagi tujuan rujukan dan audit.	CDO JPICT ICTSO

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	PERANAN
5.2.1 Peranan dan Tanggungjawab Keselamatan Maklumat Semua tanggungjawab keselamatan maklumat hendaklah ditentukan dan diperuntukkan. Setiap individu perlu memahami peranan, tanggungjawab dan kuasa yang jelas. Peranan dan tanggungjawab perlu didokumenkan, dikomunikasikan dan digunakan secara konsisten di seluruh KKM untuk memastikan pengasingan tugas yang mencukupi.	Semua
5.2.2 Peranan dan Tanggungjawab Berikut adalah senarai peranan dan tanggungjawab: (a) Ketua Setiausaha (KSU) Peranan dan tanggungjawab KSU adalah seperti berikut: (i) memastikan penguatkuasaan pelaksanaan PKS; (ii) memastikan semua pegawai KKM, pengguna, pihak ketiga dan pihak yang mempunyai urusan dengan perkhidmatan ICT KKM memahami dan mematuhi peruntukan-peruntukan di bawah polisi ini; (iii) memastikan semua keperluan KKM seperti sumber kewangan, pegawai dan perlindungan keselamatan adalah mencukupi; (iv) memastikan pengurusan risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam PKS KKM; dan' (v) melantik CDO dan ICTSO.	KSU
(b) Ketua Pegawai Digital (CDO) Peranan dan tanggungjawab CDO adalah seperti berikut: (i) memastikan PKS selaras dengan matlamat digital KKM dan mengurus risiko keselamatan dalam perubahan digital; (ii) membantu membangunkan, mengemas kini, dan melaksanakan PKS yang relevan dengan teknologi digital terkini; (iii) mendidik dan meningkatkan kesedaran keselamatan siber dalam kalangan pegawai serta memastikan penglibatan semua pihak berkepentingan; (iv) memastikan inisiatif digital mematuhi peraturan keselamatan siber dan mengawasi tadbir urus yang berkesan; (v) memastikan semua inisiatif digital dilaksanakan dengan selamat; (vi) menilai dan mengintegrasikan keselamatan dalam penggunaan teknologi digital baru tanpa menjejaskan inovasi;	CDO

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	PERANAN
(vii) membantu dalam persediaan dan tindak balas terhadap insiden keselamatan siber, serta menilai keberkesanan selepas insiden berlaku; dan	
(c) Ketua Jabatan Peranan dan tanggungjawab Ketua Jabatan adalah seperti berikut: (i) menyampaikan, menguatkuasakan dan memantau pematuhan PKS di KKM (ii) menyediakan dan memastikan semua pegawai di bawah kawalannya memahami, menghayati dan melaksanakan peruntukan yang ditetapkan di bawah polisi ini; (iii) menyediakan sumber sokongan yang diperlukan seperti pegawai, kemudahan, peralatan dan kawalan keselamatan di fasiliti; (iv) melaksanakan pengurusan risiko dan program keselamatan siber seperti yang ditetapkan di dalam PKS KKM; dan (v) menamakan pegawai yang sesuai untuk dilantik sebagai wakil keselamatan ICT di fasiliti.	Ketua Jabatan
(d) Pengurus ICT Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: (i) memastikan PKS KKM dilaksanakan dan dipatuhi; (ii) memastikan semua pengguna mematuhi dasar piawaian dan garis panduan keselamatan siber; (iii) melaksanakan keperluan PKS dalam operasi semasa seperti berikut: (a) pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu; (b) pembelian atau peningkatan perisian dan sistem komputer; (c) perolehan teknologi dan perkhidmatan komunikasi baharu; (d) pelantikan pihak ketiga, perunding atau rakan usaha sama; dan (e) menentukan pihak ketiga, perunding atau rakan usaha sama menjalani tapisan keselamatan selaras dengan keperluan tahap perkhidmatan; (iv) menyemak dan mengesahkan garis panduan, prosedur dan tatacara bagi semua aplikasi yang dibangunkan mematuhi keperluan PKS KKM;	Pengurus ICT

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	PERANAN
(v) membangun, mengkaji semula, mengemas kini pelan kontigensi dan mengaktifkan Pelan Pemulihan Bencana ICT (DRP ICT) mengikut keperluan; (vi) memastikan sistem kawalan capaian pengguna ke atas aset-aset KKM dilaksanakan; dan (vii) memastikan aspek keselamatan maklumat dilaksanakan dalam setiap pengurusan projek.	
(e) ICTSO Tanggungjawab Pegawai Keselamatan ICT (ICTSO) yang dilantik adalah seperti berikut: (i) memantau pelaksanaan PKS KKM; (ii) memberi penerangan dan pendedahan berkaitan PKS KKM kepada semua pengguna; (iii) mewujudkan garis panduan, prosedur dan tatacara selaras keperluan PKS KKM; (iv) mengurus penilaian risiko keselamatan maklumat; (v) mengurus pengauditan keselamatan maklumat merangkumi kajian semula, rumusan tindakan pengukuhan dan penyediaan laporan berdasarkan hasil penemuan; (vi) memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (vii) bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan tindakan pembaikan dan pengukuhan dengan segera; (viii) mengurus, menyedia dan melaksanakan program-program kesedaran keselamatan siber; (ix) menjalankan penilaian untuk memastikan tahap keselamatan, tindakan pemulihan dan pengukuhan keselamatan siber dilaksanakan supaya insiden baharu dapat dielakkan; dan (x) melaporkan insiden keselamatan siber kepada NC4 dan memaklumkan kepada CSIRT IPKKM.	ICTSO IPKKM
(f) ICTSO Fasiliti Peranan tanggungjawab ICTSO Fasiliti yang dilantik adalah seperti berikut: (i) melaksanakan kawalan keselamatan Siber selaras dengan keperluan KKM; (ii) memberi penerangan dan pendedahan berkenaan PKS jaatan kepada semua pengguna;	ICTSO Fasiliti

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	PERANAN
(iii) melaksanakan penilaian risiko keselamatan maklumat; (iv) melaksanakan pengurusan pengauditan keselamatan maklumat merangkumi kajian semula, rumusan tindakan pengukuhan dan penyediaan laporan berdasarkan hasil penemuan; (v) melaporkan insiden keselamatan siber kepada NC4 dan memaklumkan kepada CSIRT IPKKM; (vi) bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan tindakan pembaikan dan pengukuhan dengan segera; (vii) memantau pematuhan PKS KKM; (viii) menyedia dan melaksanakan program-program kesedaran keselamatan siber; dan (ix) menjalankan penilaian untuk memastikan tahap keselamatan, tindakan pemulihan dan pengukuhan keselamatan siber dilaksanakan supaya insiden baharu dapat dielakkan.	
(g) JPICT Peranan dan tanggungjawab JPICT seperti yang terkandung dalam **Surat Pekeliling Am Bil 3 Tahun 2015: Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT) Agensi Sektor Awam** bagi pengurusan keselamatan siber.	JPICT
(h) CSIRT Keanggotaan CSIRT ialah seperti yang berikut: i) Pengarah: Ketua Jabatan ii) Pengurus: ICTSO iii) Ahli: Pegawai Teknologi Maklumat yang dilantik Peranan dan tanggungjawab CSIRT ialah seperti yang berikut: i) Mengendalikan insiden berdasarkan garis panduan/prosedur yang telah ditetapkan; ii) Memantau, mengesan insiden, menerima dan mengesahkan aduan insiden keselamatan siber, seterusnya mengenal pasti jenis insiden serta menilai impak insiden keselamatan siber; iii) Merekodkan dan menjalankan siasatan awal terhadap insiden yang diterima; iv) Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan serta pengukuhan keselamatan siber supaya insiden baharu dapat dielakkan; v) Menyebarkan makluman/amaran berkaitan insiden kepada warga JDN; dan vi) Memastikan fail log disimpan sekurangkurangnya enam bulan di tempat yang selamat.	CSIRT

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	PERANAN
(i) Penyelaras ICT Fasiliti Peranan dan tanggungjawab Penyelaras ICT Fasiliti adalah seperti berikut: (i) melaksanakan kawalan keselamatan siber selaras polisi KKM; (ii) melaksanakan kawalan capaian kepada semua pengguna terhadap aset di fasiliti; (iii) melaporkan dan merekod sebarang perkara atau penemuan mengenai keselamatan siber kepada ICTSO Fasiliti berkenaan; dan (iv) menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan siber.	Penyelaras ICT Fasiliti
(j) Pemilik Sistem Peranan dan tanggungjawab Pemilik Sistem adalah seperti berikut: (i) pelaksanaan promosi sistem kepada pengguna sasaran; (ii) penentuan pengguna dan kategori atau tahap capaian pengguna sistem (iii) pengurusan senarai pengguna yang terlibat dengan latihan pengguna; (iv) penguatkuasaan penggunaan sistem dalam kalangan pengguna; (v) pemantauan pelaksanaan dan keberkesanan sistem secara berterusan; dan (vi) pemakluman sebarang masalah dan keperluan peningkatan sistem kepada Pembangun Sistem. Pemilik Sistem hendaklah melantik seorang pegawai sebagai Pentadbir Sistem untuk tujuan penyenggaraan/ penambahbaikan sistem yang dikendalikan tersebut.	Pemilik Sistem
(k) Pentadbir Sistem ICT Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: (i) memastikan kerahsiaan kata laluan aset ICT; (ii) mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pegawai yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; (iii) mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pengguna luar dan pihak ketiga yang berhenti atau tamat projek;	Pentadbir Sistem ICT

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	PERANAN
(iv) menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat seperti yang telah ditetapkan di dalam PKS KKM; (v) memantau aktiviti capaian harian sistem aplikasi pengguna berdasarkan keperluan sistem aplikasi; (vi) mengenal pasti dan melaporkan kepada CSIRT tentang aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; (vii) menyimpan dan menganalisis rekod jejak audit; (viii) menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat secara berkala; (ix) bertanggungjawab memantau setiap peralatan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; dan; (x) bertanggungjawab memastikan setiap perolehan perkakasan dan perisian ICT adalah tulen.	
(j) Pemilik Sistem Peranan dan tanggungjawab Pemilik Sistem adalah seperti berikut: (i) pelaksanaan promosi sistem kepada pengguna sasaran; (ii) penentuan pengguna dan kategori atau tahap capaian pengguna sistem (iii) pengurusan senarai pengguna yang terlibat dengan latihan pengguna; (iv) penguatkuasaan penggunaan sistem dalam kalangan pengguna; (v) pemantauan pelaksanaan dan keberkesanan sistem secara berterusan; dan (vi) pemakluman sebarang masalah dan keperluan peningkatan sistem kepada Pembangun Sistem. Pemilik Sistem hendaklah melantik seorang pegawai sebagai Pentadbir Sistem untuk tujuan penyenggaraan/penambahbaikan sistem yang dikendalikan tersebut.	Pemilik Sistem
(k) Pentadbir Sistem ICT Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: (i) memastikan kerahsiaan kata laluan aset ICT; (ii) mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pegawai yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; (iii) mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pengguna luar dan pihak ketiga yang berhenti atau tamat projek;	Pentadbir Sistem ICT

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	PERANAN
(iv) menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat seperti yang telah ditetapkan di dalam PKS KKM; (v) memantau aktiviti capaian harian sistem aplikasi pengguna berdasarkan keperluan sistem aplikasi; (vi) mengenal pasti dan melaporkan kepada CSIRT tentang aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; (vii) menyimpan dan menganalisis rekod jejak audit; (viii) menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat secara berkala; (ix) bertanggungjawab memantau setiap peralatan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; dan; (x) bertanggungjawab memastikan setiap perolehan perkakasan dan perisian ICT adalah tulen.	
(l) Pentadbir Rangkaian Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut: (i) mentadbir akaun pengguna; (ii) merangka, melaksana dan menguatkuasakan PKS seperti perlindungan dan perkongsian data; (iii) merancang dan melaksana polisi ancaman keselamatan, memantau keadaan rangkaian dan mengawal penggunaan sumber; (iv) pemantauan aktiviti capaian harian pengguna; (v) menyediakan laporan mengenai aktiviti capaian secara berkala; (vi) menyelia dan membuat proses sandaran pelayan; dan (vii) memberi bantuan dan khidmat nasihat teknikal dalam menyelesaikan masalah-masalah berkaitan rangkaian yang dilaporkan oleh pengguna.	Pentadbir Rangkaian
(m) Pengguna Peranan dan tanggungjawab pengguna adalah seperti berikut: (i) membaca, memahami dan mematuhi PKS KKM; (ii) mengetahui dan memahami implikasi keselamatan siber, kesan dari tindakannya;	Pengguna

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	PERANAN
(iii) menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; (iv) mematuhi prinsip-prinsip PKS dan menjaga kerahsiaan maklumat KKM; (v) melaksanakan langkah-langkah perlindungan seperti berikut: a) menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) memeriksa maklumat dan mengesahkan ia tepat dan lengkap dari semasa ke semasa; c) menentukan maklumat sedia untuk digunakan; d) menjaga kerahsiaan kata laluan; e) mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f) memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan penghapusan; dan g) menjaga kerahsiaan langkah-langkah keselamatan siber dari diketahui umum. h) melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO IPKKM atau ICTSO Fasiliti berkenaan dengan segera; (vi) menghadiri program-program kesedaran keselamatan siber; dan (vii) menandatangani Surat Akuan Pematuhan PKS KKM melalui Sistem Akuan Pematuhan (ePatuh) atau secara manual.	
5.3 PENGASINGAN TUGAS (SEGREGATION OF DUTIES)	**PERANAN**
5.3.1 Pengasingan Tugas dan Bidang Tanggungjawab Pengasingan tugas dan bidang tanggungjawab dilaksanakan bagi mengurangkan peluang pengubahsuaian data dan maklumat tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset. Sekiranya tiada pemisahan tugas dan tanggungjawab yang betul, penipuan, penyalahgunaan, capaian tanpa kebenaran dan isu keselamatan lain mungkin akan timbul. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset; (b) tugas mewujud, menghapus, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi;	Pengurus ICT Ketua Jabatan

5.3 PENGASINGAN TUGAS (SEGREGATION OF DUTIES)	PERANAN
(c) perkakasan yang digunakan bagi aktiviti membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai produksi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan (d) pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.	
5.3.2 Aktiviti yang Memerlukan Pengasingan Terdapat beberapa aktiviti yang dikenal pasti memerlukan pengasingan semasa pelaksanaan antaranya adalah seperti berikut: (a) memula, melulus dan melaksana perubahan; (b) memohon, melulus dan melaksanakan hak capaian; (c) mereka bentuk, melaksana dan menyemak kod sumber; (d) membangunkan perisian dan mentadbir sistem; (e) mengguna aplikasi dan mentadbir aplikasi; (f) mengguna aplikasi dan mentadbir pangkalan data; dan (g) mereka bentuk, mengaudit dan memastikan kawalan keselamatan maklumat. Jika kawalan sedemikian tidak dapat dilakukan, terutamanya untuk jabatan kecil, pemantauan aktiviti, jejak audit dan penyeliaan pengurusan boleh digunakan. Jabatan yang lebih besar boleh menggunakan alatan automasi untuk mengenal pasti dan mengasingkan peranan bagi mengelakkan percanggahan peranan.	Pengurus ICT Ketua Jabatan
5.4 TUGAS DAN TANGGUNGJAWAB PENGURUSAN *(MANAGEMENT RESPONSIBILITIES)*	**PERANAN**
5.4.1 Tanggungjawab Pengurusan Pelaksanaan PKS akan dilaksanakan oleh Ketua Setiausaha dengan disokong oleh JPICT yang terdiri daripada Pengarah Bahagian, Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO), Ketua Jabatan dan ahli-ahli lain yang dilantik. Perkara yang perlu dipatuhi adalah seperti berikut: (a) peranan pegawai dan pihak ketiga hendaklah diberi berdasarkan keperluan dan kompetensi masing-masing; (b) setiap pegawai KKM dan pihak ketiga yang terlibat dengan Maklumat Rahsia Rasmi hendaklah menandatangani perjanjian ketidakdedahan; dan (c) tiada had capaian diberikan kepada individu sebelum kelulusan tapisan keselamatan bagi yang berurusan dengan Maklumat Rahsia Rasmi. PKS mestilah dipatuhi oleh semua pegawai, pembekal, pihak ketiga dan pihak yang mempunyai urusan dengan perkhidmatan ICT di KKM. Perkara yang perlu dipastikan adalah seperti berikut:	KSU CDO ICTSO Pengurus ICT Ketua Jabatan

5.4 TUGAS DAN TANGGUNGJAWAB PENGURUSAN *(MANAGEMENT RESPONSIBILITIES)*	PERANAN
(a) tanggungjawab dan peranan dalam keselamatan maklumat sebelum capaian diberikan kepada maklumat KKM; (b) menerima garis panduan yang menentukan tahap keselamatan maklumat yang dijangkakan dalam peranan khas tugas; (c) memenuhi semua polisi, garis panduan atau arahan keselamatan maklumat KKM yang berkuatkuasa; (d) sedar akan peranan dan tanggungjawab berkaitan keselamatan maklumat; (e) mematuhi kepada peraturan tempat kerja, termasuk segala polisi, garis panduan atau arahan keselamatan maklumat KKM yang berkuatkuasa; dan (h) memastikan sumber dan masa perancangan projek mencukupi untuk melaksanakan proses berkaitan keselamatan dan kawalan PKS.	
5.5 HUBUNGAN DENGAN PIHAK BERKUASA *(CONTACT WITH AUTHORITIES)*	**PERANAN**
5.5.1. Mengenal Pasti dan Mengemas kini Maklumat Pihak Berkuasa KKM perlu mewujudkan dan mengekalkan hubungan dengan pihak berkuasa yang berkaitan. KKM hendaklah memastikan senarai perhubungan dengan pelbagai pihak yang berkaitan diwujud dan dikemas kini. Ia merupakan sumber rujukan pengguna KKM untuk mengetahui senarai perhubungan pihak berkuasa yang berdekatan. KKM perlu mengenal pasti siapa yang perlu dihubungi, contohnya, penguatkuasa undang-undang, badan kawal selia dan pihak berkuasa penyeliaan seperti Majlis Keselamatan Negara (MKN), *National Cyber Security Agency* (NACSA), Jabatan Digital Negara (JDN), Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) dan sebagainya.	Pengurus ICT Penyelaras ICT Fasiliti Pemilik Sistem
5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN *(CONTACT WITH SPECIAL INTEREST GROUPS)*	**PERANAN**
5.6.1. Hubungan dengan Kumpulan Berkepentingan yang Khusus Kawalan ini memastikan bahawa keselamatan maklumat sampai kepada kumpulan berkepentingan sama ada pengguna, pihak ketiga dan sebagainya. Perkongsian membolehkan semua pihak mendapat manfaat bersama dari segi pengetahuan, idea dan amalan terbaik. KKM perlu mewujudkan dan mengekalkan hubungan dengan kumpulan berkepentingan bagi mendapat manfaat berikut : (a) meningkatkan ilmu berkaitan amalan terbaik; (b) mengikuti perkembangan terkini mengenai keselamatan maklumat; (c) menerima amaran awal dan nasihat berhubung ancaman keselamatan maklumat terkini; (d) berkongsi dan bertukar maklumat mengenai teknologi, produk atau ancaman;	ICTSO IPKKM ICTSO FASILITI CSIRT KKM

5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN *(CONTACT WITH SPECIAL INTEREST GROUPS)*	PERANAN
(e) berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat;dan (f) mendapat nasihat pakar tentang keselamatan maklumat.	
5.7 PERISIKAN ANCAMAN *(THREAT INTELLIGENCE)*	**PERANAN**
5.7.1 Perisikan Ancaman Maklumat berkaitan ancaman keselamatan maklumat perlu dikumpulkan dan dianalisis untuk menghasilkan maklumat perisikan ancaman. Perisikan ancaman digunakan untuk mencegah, mengesan atau bertindak balas terhadap ancaman yang menyebabkan kemudaratan kepada KKM.	CSIRT IPKKM CSIRT Fasiliti KKM Pemilik Sistem
5.7.2 Taktik, Teknik dan Prosedur (TTP) Perisikan ancaman yang biasa digunakan untuk melaksanakan serangan adalah Taktik, Teknik dan Prosedur (TTP). Pemahaman tentang TTP adalah penting dalam usaha mempertahankan rangkaian dan sistem maklumat kerana ia membantu KKM mengenal pasti dan bertindak balas kepada ancaman dengan lebih berkesan. KKM perlu melaksanakan perkara berikut: (a) menyemak ancaman secara berkala (dengan menyemak laporan daripada agensi kerajaan dan organisasi lain); (b) sumber ancaman terdiri dari orang dalam, pesaing, penjenayah, kumpulan pengganas yang perlu dikenal pasti; (c) tentukan kemungkinan vektor serangan baharu dan berdasarkan peristiwa semasa atau kejadian lalu; dan (d) membina pertahanan yang akan membantu mengurangkan ancaman keselamatan kepada KKM.	CSIRT IPKKM CSIRT Fasiliti KKM Pemilik Sistem
5.7.3 Syor Perisikan Ancaman Pertubuhan Piawaian Antarabangsa (ISO) mengesyorkan supaya KKM mengambil kira ketiga-tiga peringkat perisikan, iaitu strategik, taktikal dan operasi, supaya boleh memanfaatkan perisikan ancaman dengan berkesan: **(a) Perisikan Ancaman Strategik** Pertukaran maklumat peringkat tinggi tentang landskap ancaman yang berkembang seperti jenis penyerang dan serangan. **(b) Perisikan Ancaman Taktikal:** Perisikan tentang alatan, teknik dan metodologi serangan. **(c) Perisikan Ancaman Operasi** Perisikan mengenai pengetahuan tentang taktik, serangan khusus dan penunjuk.	CSIRT IPKKM CSIRT Fasiliti KKM Pemilik Sistem

5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK *(INFORMATION SECURITY IN PROJECT MANAGEMENT)*	PERANAN
5.8.1 Keselamatan Maklumat dalam Pengurusan Projek Keselamatan maklumat hendaklah diberi perhatian dalam pengurusan projek bagi memastikan risiko keselamatan maklumat yang berkaitan dengan projek dan penyampaian dapat diurus dengan berkesan. Keselamatan maklumat perlu dijadikan sebagai sebahagian daripada proses perancangan dan pelaksanaan projek. Perkara-perkara berikut perlu dipatuhi seperti berikut: (a) semua ahli projek perlu memahami kepentingan keselamatan maklumat dan mematuhinya; (b) menentukan keperluan keselamatan maklumat dalam projek dengan mengambil kira keperluan perkhidmatan dan keperluan undang-undang; (c) ancaman keselamatan maklumat perlu dinilai dari segi kesan risikonya; (d) mengurus kesan risiko, laksana kawalan dan proses yang sesuai; (e) memastikan kawalan ini dipantau dan dilaporkan secara berkala; dan (f) Peranan dan tanggungjawab keselamatan maklumat projek hendaklah ditakrifkan dan ditentukan.	Pengarah Projek Pengurus Projek Pemilik Sistem
5.8.2 Keperluan dalam Keselamatan Maklumat Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek tanpa mengira kerumitan, saiz, tempoh serta bidang. Perkara yang perlu dipatuhi semasa pengurusan projek adalah seperti berikut: (a) keselamatan maklumat perlu diambil kira dalam setiap projek yang melibatkan ICT; (b) objektif keselamatan maklumat hendaklah diambil kira dalam semua fasa pelaksanaan projek; (c) penilaian risiko keselamatan maklumat hendaklah dikendalikan di awal projek bagi mengenal pasti kawalan-kawalan yang diperlukan, contohnya, keperluan keselamatan aplikasi (8.26), keperluan untuk mematuhi hak harta intelek (5.32); (d) kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam PKS; (e) penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pensijilan minimum keselamatan maklumat bagi pasukan projek; (f) keselamatan maklumat hendaklah dilaksanakan berdasarkan kawalan, akta, dasar atau pekeliling yang sedang berkuatkuasa; (g) sebagai sebahagian daripada kitaran hayat projek, risiko keselamatan maklumat yang berkaitan dengan pelaksanaan projek perlu dipertimbangkan dan ditangani. Ini termasuk keselamatan saluran komunikasi dalaman dan luaran; dan (h) menjalankan penilaian dan ujian keberkesanan terhadap pemulihan risiko keselamatan maklumat.	Pengarah Projek Pengurus Projek Pemilik Sistem

5.9 INVENTORI MAKLUMAT DAN ASET BERKAITAN YANG LAIN *(INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS)*	PERANAN
5.9.1 Inventori Aset Aset yang dikaitkan dengan maklumat dan kemudahan pemprosesan maklumat hendaklah dikenal pasti dan inventori aset ini hendaklah disediakan dan diselenggara. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara perkara berikut: (a) memastikan semua aset dikenal pasti, di kelas (di kategori), di dokumen, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemas kini sebagaimana arahan dan peraturan semasa yang berkuatkuasa; (b) memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; (c) pegawai aset hendaklah mengesahkan penempatan aset ICT yang ditempatkan; dan (d) setiap pengguna adalah bertanggungjawab ke atas semua aset di bawah kawalannya.	Pegawai Aset Pegawai Penerima Aset Pengguna
5.9.2 Pemilikan Aset Aset hak milik KKM hendaklah diselenggara mengikut jadual penyelenggaraan yang ditetapkan serta mematuhi Pekeliling berkaitan Pengurusan Aset Kerajaan. Aset bukan hakmilik KKM hendaklah didaftarkan dan diurus mengikut prosedur/arahan-arahan atau polisi Bring Your Own Device (BYOD) yang sedang berkuatkuasa. Tanggungjawab yang perlu dipatuhi oleh pemilik aset merangkumi perkara yang berikut: (a) memastikan aset didaftarkan dalam senarai aset mengikut pengelasan sebelum diserahkan kepada pemilik aset; (b) memastikan aset dilindungi mengikut pengelasan yang tepat; (c) memastikan pengelasan aset disemak secara berkala untuk memastikan ketepatannya; (d) aset tidak ketara juga perlu direkodkan termasuk pangkalan data, storan, komponen perisian dan sub-komponen; (f) menghadkan capaian bersesuaian mengikut pengelasan aset untuk memastikan perlindungan berterusan; (g) maklumat dan aset dapat dikendalikan dengan cara yang selamat apabila ia dipadamkan atau dilupuskan dan dikeluarkan daripada senarai aset; (h) pengguna bertanggungjawab untuk mengenal pasti dan mengendalikan risiko yang berkaitan dengan aset; (i) pengguna perlu memberikan kerjasama kepada pegawai yang diberikan tanggungjawab untuk menguruskan maklumat aset; dan (j) Aset bukan hakmilik KKM hendaklah didaftarkan dan diurus mengikut prosedur/arahan-arahan atau polisi *Bring Your Own Device* (BYOD) yang sedang berkuatkuasa.	Pengarah Projek Pengurus Projek Pemilik Sistem

5.9 INVENTORI MAKLUMAT DAN ASET BERKAITAN YANG LAIN *(INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS)*	PERANAN
5.9.3 Pengelasan Maklumat Aset Memastikan setiap maklumat aset dikelaskan mengikut pengelasan dan peringkat keselamatan dokumen selaras dengan Akta Rahsia Rasmi 1972, Arahan Keselamatan, polisi, garis panduan, arahan atau lain-lain yang berkaitan yang sedang berkuatkuasa.	Pegawai Aset Pegawai Penerima Aset Pengguna
5.10 PENGGUNAAN YANG DITERIMA BAGI MAKLUMAT DAN ASET BERKAITAN YANG LAIN *(ACCEPTABLE USE OF INFORMATION AND OTHER ASSOCIATED ASSETS)*	**PERANAN**
5.10.1 Penggunaan Aset yang Dibenarkan Memastikan penggunaan aset untuk tujuan rasmi serta mengikut fungsi yang telah ditetapkan oleh KKM.	Pengguna Pihak ketiga Pegawai KKM
5.10.2 Pengendalian Aset Tanggungjawab yang perlu dipatuhi oleh pegawai, pihak ketiga dan pengguna bagi melindungi dan mengendalikan aset dan maklumat adalah seperti berikut: (a) merujuk kepada arahan dan peraturan semasa yang berkuatkuasa meliputi Penerimaan, Pendaftaran, Penggunaan, Penyimpanan, Pemeriksaan, Penyelenggaraan, Pelupusan, Kehilangan dan Hapus Kira; (b) merujuk kepada prosedur dalam KKM, arahan keselamatan terkini dan lain-lain yang berkaitan; (c) pelaksanaan ke ruang storan pengkomputeran awan perlu dirujuk berdasarkan kawalan, akta, dasar atau pekeliling yang sedang berkuatkuasa yang berkaitan. (d) sekatan capaian untuk menyokong perlindungan pada setiap tahap keselamatan mesti dilaksanakan; (e) mengekalkan daftar pengguna yang dibenarkan/disahkan ke atas maklumat dan lain-lain aset yang berkaitan; (f) memastikan keselamatan maklumat sama ada salinan asal atau salinan sementara adalah konsisten dengan keperluan; (g) memastikan pemeliharaan data dari awal diutamakan; (h) memastikan penyimpanan aset berkaitan maklumat hendaklah mematuhi spesifikasi penyimpanan yang ditetapkan oleh pengeluar/ kilang; (i) melabel semua salinan media storan elektronik atau fizikal dengan jelas untuk perhatian penerima; dan (j) mengesahkan pelupusan maklumat dan lain-lain aset mengikut peraturan, arahan, polisi atau lain-lain yang sedang berkuatkuasa.	Pengguna Pihak ketiga Pegawai KKM
5.11 PEMULANGAN ASET *(RETURN OF ASSETS)*	**PERANAN**
5.11.1 Pemulangan Aset Aset maklumat KKM mempunyai nilai dalam pelbagai segi. Ini termasuk mengandungi maklumat sensitif tentang pengguna, pegawai atau pihak berkepentingan lain yang boleh dieksploitasi oleh orang yang tidak bertanggungjawab untuk keuntungan peribadi.	Pengguna Pegawai Aset Pemilik Aset

5.11 PEMULANGAN ASET *(RETURN OF ASSETS)*	PERANAN
Atas sebab ini, semua aset pegawai dan pihak ketiga yang menamatkan perkhidmatan dengan KKM mesti dipulangkan. Sebagai sebahagian daripada polisi keluar *(asset's exit policy)*, aset perlu dipulangkan mengikut arahan, garis panduan, atau lain-lain peraturan yang sedang berkuatkuasa. Antara perkara yang turut perlu dipertimbangkan adalah seperti berikut: (a) memastikan perlindungan yang berterusan, audit aset berkala juga perlu untuk memastikan prosedur pemulangan aset tetap dan terancang; (b) pegawai KKM dan pihak-pihak lain yang berkepentingan perlu mengembalikan semua aset KKM yang berada di dalam milikan apabila terdapat perubahan atau penamatan perkhidmatan, kontrak, atau perjanjian; (c) Individu tanpa kebenaran adalah dilarang daripada menyimpan aset KKM (termasuk peralatan, maklumat, perisian, dsb.); (d) KKM mesti memastikan pekerja dan kontraktor tidak mengambil data sensitif dengan mengenal pasti potensi ancaman dan memantau aktiviti pengguna sebelum keluar/ selesai terhadap kerja-kerja dijalankan. (e) proses penamatan rasmi perlu diwujudkan oleh KKM supaya individu tidak lagi boleh mencapai mana-mana sistem ICT. KKM boleh membatalkan semua kebenaran, menyahaktif akaun dan mengalih keluar capaian daripada premis bangunan; (f) KKM perlu menyemak kawasan kerja individu untuk memastikan semua maklumat sensitif telah dikembalikan; (g) proses perubahan atau penamatan perlu formal, termasuk memulangkan semua aset fizikal dan elektronik yang dikeluarkan sebelum ini yang dimiliki atau diamanahkan kepada individu; (h) Sebarang hak capaian, akaun, sijil digital dan kata laluan juga perlu dipinda sebagai sebahagian daripada proses. Pembentukan ini amat kritikal apabila perubahan atau penamatan berlaku secara tidak dijangka, seperti kematian atau peletakan jawatan. Capaian tanpa kebenaran kepada aset KKM boleh menyebabkan pelanggaran data jika tidak dicegah. (i) Semua aset pengguna yang telah bersara, bertukar jabatan atau menamatkan perkhidmatan atau kontrak dengan KKM mesti dipulangkan. (j) Aset perlu dipulangkan mengikut arahan, garis panduan, atau lain-lain peraturan yang sedang berkuatkuasa.	
5.12 PENGELASAN MAKLUMAT *(CLASSIFICATION OF INFORMATION)*	**PERANAN**
5.12.1 Pengelasan Maklumat Data dan maklumat perlu di kelas oleh Pegawai Pengelas yang diberi kuasa. Maklumat hendaklah dikelaskan sewajarnya mengikut keperluan keselamatan maklumat yang telah ditetapkan dalam Akta Rahsia Rasmi 1972, Arahan Keselamatan, Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan dan lain-lain peraturan yang berkuatkuasa	Ketua Jabatan Pegawai Pengelas Pemilik Aset

5.12 PENGELASAN MAKLUMAT *(CLASSIFICATION OF INFORMATION)*	**PERANAN**
Pengkelasan maklumat terdiri daripada aktiviti penentuan pengelasan maklumat serta penentuan peringkat keselamatan maklumat. Pengelasan maklumat terdiri daripada maklumat rahsia rasmi dan maklumat rasmi manakala peringkat keselamatan maklumat terdiri daripada rahsia besar, rahsia, sulit terhad, data terkawal/sensitif dan terbuka. Pelaksanaan kawalan ini membolehkan KKM: (a) mengenal pasti risiko dengan menentukan tahap perlindungan yang sesuai untuk setiap aset maklumat berdasarkan kepentingan dan sensitiviti; (b) memberi perhatian terhadap pengelasan maklumat yang berlebihan atau kurang; (c) mempertimbangkan kerahsiaan, ketersediaan dan keperluan integriti apabila memperuntukkan aset kepada kategori masing-masing. (d) membantu untuk memastikan bahawa skema pengelasan mengimbangi keperluan perkhidmatan untuk maklumat dan keperluan keselamatan untuk setiap kategori maklumat. (e) mempertimbangkan keperluan perkhidmatan untuk berkongsi dan menggunakan maklumat, serta keperluan untuk ketersediaan maklumat tersebut. Walau bagaimanapun, mengelaskan aset maklumat boleh mengganggu fungsi perkhidmatan kritikal dengan menyekat capaian kepada dan penggunaan maklumat; dan (f) perlu mengimbangi keperluan perkhidmatan khusus untuk ketersediaan dan penggunaan data dan keperluan untuk mengekalkan kerahsiaan dan integriti maklumat tersebut.	
5.12.2 Kerahsiaan, integriti dan Ketersediaan Maklumat KKM perlu menekankan keperluan menjaga kerahsiaan, integriti dan ketersediaan maklumat apabila mengkategorikan aset maklumat. Perkara yang boleh dipertimbangkan adalah seperti berikut: (a) mengguna pakai pendekatan *risk-based* bagi menilai potensi kesan daripada pelanggaran keselamatan atau kompromi ke atas aset maklumat. (b) mengenalpasti potensi kesan yang menjejaskan kerahsiaan, integriti atau ketersediaan maklumat itu terhadap KKM; (c) tahap perlindungan yang diperlukan oleh setiap kategori maklumat dan memperuntukkan sumber dengan sewajarnya. (d) setiap bentuk maklumat mempunyai tahap kepentingan yang unik kepada fungsi KKM dan mempunyai tahap sensitiviti yang berbeza-beza bergantung pada keadaan tertentu; (e) apabila KKM melaksanakan skema pengelasan maklumat, ia harus mempertimbangkan potensi kesan yang menjejaskan kerahsiaan, integriti atau ketersediaan maklumat itu terhadap KKM; Sensitiviti dan potensi kesan pangkalan data yang mengandungi alamat e-mel individu pengurusan profesional yang berpengaruh akan jauh berbeza daripada rekod kesihatan pekerja. Oleh itu, KKM perlu mempertimbangkan dengan teliti tahap perlindungan yang diperlukan oleh setiap kategori maklumat dan memperuntukkan sumber dengan sewajarnya.	Ketua Jabatan Pegawai Pengelas Pemilik Aset

5.12 PENGELASAN MAKLUMAT *(CLASSIFICATION OF INFORMATION)*	**PERANAN**
5.12.3 Mengemas kini dan menyemak pengelasan secara berkala Nilai, kepentingan dan tahap sensitiviti maklumat boleh berubah dari semasa ke semasa apabila data melalui kitaran hayatnya. Oleh itu, KKM perlu sentiasa menyemak pengelasan maklumat dan membuat pengemaskinian yang diperlukan.	Ketua Jabatan Pegawai Pengelas Pemilik Aset
5.12.4 Skema pengelasan maklumat Sekiranya tiada kaedah pengelasan yang boleh digunakan secara umum, KKM mempunyai fleksibiliti untuk menubuhkan dan menentukan tahap pengelasan. Perkara yang boleh dipertimbangkan semasa pengelasan maklumat adalah seperti berikut: (a) pendedahannya tidak mendatangkan mudarat; (b) pendedahannya menyebabkan kerosakan reputasi kecil atau kesan operasi kecil; (c) pendedahannya mempunyai kesan jangka pendek yang ketara ke atas operasi atau objektif perkhidmatan; dan (d) pendedahannya memberi kesan serius kepada objektif perkhidmatan jangka panjang atau mempertaruhkan kelangsungan perkhidmatan KKM.	Ketua Jabatan Pegawai Pengelas Pemilik Aset
5.13 PELABELAN MAKLUMAT *(LABELLING OF INFORMATION)*	**PERANAN**
Semua maklumat yang ditandakan sebagai terperingkat hendaklah mematuhi Arahan Keselamatan: Keselamatan Rahsia Rasmi dan semua maklumat yang dikelaskan terperingkat dalam format elektronik hendaklah mematuhi Arahan Keselamatan: Keselamatan Rahsia Rasmi Dalam Persekitaran Teknologi Maklumat dan Komunikasi (ICT).	Pegawai Rekod Pegawai Pengelas Pegawai Aset Pemilik Sistem
5.14 PEMINDAHAN MAKLUMAT *(INFORMATION TRANSFER)*	**PERANAN**
5.14.1 Polisi dan Prosedur Pemindahan Data dan Maklumat Memastikan keselamatan perpindahan/ pertukaran data, maklumat dan perisian antara dan pihak luar terjamin dengan merujuk pada Dasar Perkongsian Data Sektor Awam dan Dasar Perkongsian Data Nasional. Pihak luar ialah pihak yang menggunakan atau pihak yang membekalkan data, maklumat atau perisian. Perkara yang perlu dipatuhi seperti berikut: (a) polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; (b) terma pemindahan data, maklumat dan perisian antara KKM dengan pihak luar hendaklah dimasukkan dalam perjanjian pertukaran data, maklumat atau perisian; (c) media yang mengandungi data, maklumat dan perisian perlu dilindungi; dan (d) memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.	Pengurus ICT Pemilik Sistem Penyelaras ICT Fasiliti




“Kejahilan dalam isu keselamatan siber lebih tinggi kosnya berbanding mana-mana solusi teknologi.”
- Dan Geer

5.14 PEMINDAHAN MAKLUMAT *(INFORMATION TRANSFER)*	PERANAN
5.14.2 Perjanjian Mengenai Pemindahan Data dan Maklumat Semua pihak yang terlibat perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara KKM dengan pihak luar serta mematuhi Dasar Perkongsian Data Sektor Awam dan Dasar Perkongsian Data Nasional. Perkara yang perlu dipertimbangkan ialah: Perkara yang perlu dipertimbangkan dalam pemindahan maklumat adalah seperti berikut: (a) menentukan kawalan yang sesuai berdasarkan tahap pengelasan maklumat untuk melindunginya semasa dalam transit daripada capaian tanpa kebenaran, pengubahan, pemintasan, penduaan, penghapusan dan serangan *DOS/ DDOS*; (b) berupaya untuk menjejaki semasa data dalam transit dan mewujudkan serta menjalankan kawalan untuk menjamin data boleh dikesan; (c) menentukan pihak yang terlibat dalam pemindahan data dan hubungan sesama pihak, seperti pemilik data dan pegawai keselamatan; (d) sekiranya berlaku pelanggaran data, liabiliti hendaklah dikenal pasti; (e) menyemak kesan ke atas undang-undang, peraturan atau arahan lain yang berkaitan pemindahan; (f) Mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data; (g) Menghadkan capaian pembekal, pegawai dan pengguna pihak luar kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat; dan (h) Memastikan dokumen perjanjian diwujudkan antara KKM dengan pihak ketiga bagi pemindahan maklumat melibatkan pihak ketiga.	Pengurus ICT Pemilik Sistem Penyelaras ICT Fasiliti
5.14.3 Pemindahan Data dan Maklumat Elektronik Pemindahan maklumat perlu mengikut Arahan Keselamatan, Akta Rahsia Rasmi, prosedur, arahan, atau lain-lain yang sedang berkuatkuasa. Perkara berikut perlu dipertimbangkan apabila memindahkan maklumat secara elektronik seperti berikut: (a) menggunakan teknologi terkini bagi mengenal pasti, menggagalkan, dan mencegah serangan perisian hasad; (b) memastikan keselamatan maklumat sulit yang terdapat dalam lampiran yang dihantar; (c) memastikan komunikasi dihantar kepada penerima yang sesuai dengan mengelakkan risiko menghantar ke alamat e-mel, alamat atau nombor telefon yang salah; (d) mendapatkan kebenaran sebelum mula menggunakan mana-mana perkhidmatan komunikasi awam; (e) kaedah pengesahan yang lebih ketat harus digunakan semasa menghantar data melalui rangkaian awam;	Pengurus ICT Pemilik Sistem Penyelaras ICT Fasiliti

5.14 PEMINDAHAN MAKLUMAT *(INFORMATION TRANSFER)*	PERANAN
(f) mengenakan had ke atas penggunaan perkhidmatan e-komunikasi, Contoh: melarang pemajuan e-mel secara automatik; (g) menasihatkan pegawai untuk mengelak daripada menggunakan perkhidmatan pesanan ringkas atau mesej segera untuk berkongsi data sensitif, kerana kandungan itu boleh dilihat oleh individu yang tidak dibenarkan di kawasan awam; dan (h) menasihatkan pegawai dan pihak lain yang berkepentingan tentang risiko perlindungan yang mungkin ditimbulkan oleh mesin faks, Contoh : capaian yang tidak dibenarkan atau salah hala mesej ke nombor tertentu.	
5.14.4 Pemindahan Data dan Maklumat Secara Verbal Pegawai mesti dimaklumkan tentang risiko yang berkaitan dengan pertukaran maklumat dalam KKM atau penghantaran data kepada pihak ketiga. Risiko termasuk perkara berikut: (a) pegawai perlu mengelak daripada membincangkan perkara sulit di saluran awam yang tidak selamat atau di kawasan awam; (b) pegawai tidak sepatutnya meninggalkan mel suara dengan maklumat sulit kerana merbahaya jika dimainkan semula oleh mereka yang tidak dibenarkan; (c) individu, pegawai dan pihak ketiga yang terlibat, perlu disaring sebelum dibenarkan masuk ke perbincangan; (d) pihak KKM yang menggunakan bilik untuk perbualan sulit hendaklah dipastikan bilik tersebut dilengkapi dengan mekanisme kalis bunyi yang diperlukan; dan (e) sebelum terlibat dalam sebarang dialog sensitif, dokumen penafian perlu ditandatangani.	Pengurus ICT Pemilik Sistem Penyelaras ICT Fasiliti
5.15 KAWALAN CAPAIAN *(ACCESS CONTROL)*	**PERANAN**
5.15.1 Polisi Kawalan Capaian Polisi khusus mengenai kawalan capaian yang selamat ke atas data adalah sangat penting bagi meminimumkan risiko capaian tanpa kebenaran ke atas sumber dan data. Selain itu, capaian merentas KKM turut perlu ditetapkan melalui kawalan capaian yang lebih khusus dan disasarkan pada fungsi perkhidmatan mengikut fasiliti/projek/program tertentu. Kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Kawalan capaian perlu disemak, dikemas kini dan disahkan sekurang-kurangnya sekali dalam tempoh setahun atau mengikut keperluan sekiranya terdapat perubahan serta menyokong peraturan kawalan capaian pengguna sedia ada. Perkara yang perlu dipertimbangkan dalam menentukan kawalan capaian adalah seperti berikut: (a) mengenal pasti entiti yang memerlukan capaian terhadap aset dan maklumat;	Pengurus ICT Penyelaras ICT Fasiliti Pentadbir Sistem Pentadbir Rangkaian

5.15 KAWALAN CAPAIAN *(ACCESS CONTROL)*	PERANAN
(b) menyelenggara rekod berkaitan peranan pengguna dan hak capaian data berdasarkan keperluan untuk memastikan pematuhan; (c) keselamatan dan integriti aplikasi yang berkaitan (rujuk Bab 8); (d) penilaian risiko boleh dijalankan untuk menilai ciri keselamatan sistem/aplikasi; (e) kawalan capaian fizikal di tapak (rujuk Bab 7); (f) kawalan capaian ke atas bangunan dan bilik, perlu dilaksanakan merangkumi sistem yang diguna pakai, kawalan perimeter dan prosedur pelawat mengikut kesesuaian; (g) apabila berkaitan dengan pengedaran, keselamatan dan pengkategorian maklumat, prinsip "perlu untuk tahu" perlu digunakan (rujuk Bab 5); (h) pihak ketiga perlu mematuhi dasar amalan terbaik yang tidak membenarkan capaian penuh kepada data merentas KKM; (i) memastikan sekatan kepada capaian istimewa dihadkan dan diurus dengan baik (j) keistimewaan capaian pengguna yang diberi melebihi hak pengguna standard mesti dipantau dan diaudit; (k) memastikan pematuhan ke atas perundangan berkaitan, garis panduan, kawal selia, atau perjanjian (kontrak) yang berkaitan dengan capaian data (rujuk Bab 5 dan 8); (l) memberi perhatian berkaitan konflik berkepentingan (conflict of interest); (m) melaksanakan proses kebenaran rasmi yang diperlukan dan didokumenkan; (n) menguruskan hak capaian secara berterusan (Bab 5); (o) audit berkala, pengawasan sumber manusia (pegawai keluar, dsb.) dan perubahan bidang tugas (Contoh: perpindahan jabatan dan perubahan kepada peranan) dilaksanakan untuk mengekalkan integriti data dan perimeter keselamatan; dan (p) Rekod log capaian pengguna hendaklah disimpan.	
5.16 PENGURUSAN IDENTITI *(IDENTITY MANAGEMENT)*	**PERANAN**
5.16.1 Pengurusan Identiti Pengguna Kawalan ini menerangkan cara untuk mengenal pasti siapa (pengguna, kumpulan pengguna) atau apakah (aplikasi, sistem dan peranti) yang mencapai data dan cara identiti tersebut diberikan hak capaian. Perkara yang perlu dipertimbangkan adalah seperti berikut: (a) setiap kali identiti diberikan, hanya orang itu sahaja yang boleh mengesahkan dengan identiti itu dan/atau menggunakannya apabila mencapai sumber dari rangkaian; (b) menetapkan dengan jelas bahawa pengguna tidak boleh berkongsi maklumat log masuk, atau membenarkan pengguna lain meneroka rangkaian menggunakan sebarang identiti selain daripada yang telah diberikan; (c) set keperluan operasi yang jelas perlu dinyatakan sekiranya terdapat keperluan untuk memberikan identiti tunggal kepada beberapa orang (berkongsi identiti);	Pentadbir Sistem ICT Pentadbir Sistem Aplikasi Pentadbir Keselamatan Pentadbir Rangkaian Pentadbir Server Pentadbir Laman Web Pentadbir E-mel Pentadbir Pangkalan Data Pentadbir Aset Pentadbir Pusat Data

5.16 PENGURUSAN IDENTITI *(IDENTITY MANAGEMENT)*	PERANAN
(d) untuk mencapai pematuhan, pendaftaran identiti berkongsi hendaklah dikendalikan secara berasingan daripada pendaftaran pengguna tunggal dengan melalui satu proses kelulusan yang khusus; (e) entiti 'bukan manusia' (sebarang identiti yang tidak terikat dengan orang sebenar) perlu diurus secara berbeza daripada identiti berasaskan pengguna semasa pendaftaran; (f) identiti bukan manusia juga perlu mempunyai kelulusan dan proses pendaftarannya sendiri; (g) sekiranya berlaku pelepasan(jawatan), meninggal dunia, aset berlebihan atau identiti lain yang tidak diperlukan, pentadbir rangkaian perlu menyahaktifkan identiti sepenuhnya; (h) akaun pengguna boleh dibekukan atau ditamatkan apabila menerima arahan daripada Bahagian Pengurusan Sumber Manusia atas sebab-sebab yang berikut: a. pengguna bercuti panjang dalam tempoh waktu melebihi tiga bulan; b. bertukar bidang tugas; c. bertukar ke jabatan lain; d. bersara; e. bagi menjalankan siasatan; atau f. ditamatkan perkhidmatan. Pentadbir sistem boleh membeku dan menamatkan identiti pengguna dengan/tanpa notis atas sebab-sebab berikut: (a) pengguna yang tidak aktif dalam masa minima sembilan puluh (90) hari atau sepertimana tempoh masa aktif minima yang ditetapkan; (b) bertukar bidang tugas kerja; (c) bertukar ke agensi lain; (d) bersara; (e) ditamatkan perkhidmatan (pembatalan serta merta); (f) dalam prosiding dan/atau dikenakan tindakan tatatertib: (pembatalan serta merta);; dan (g) meninggal dunia.	
5.17 PENGESAHAN MAKLUMAT *(AUTHENTICATION INFORMATION)*	**PERANAN**
5.17.1 Pengesahan Maklumat Identiti Pengguna Perkara yang perlu dipertimbangkan dalam melindungi hak capaian pengguna daripada capaian tanpa kebenaran adalah seperti berikut: (a) menyediakan kata laluan dan soalan keselamatan; (b) sistem yang digunakan berada dalam persekitaran yang selamat; (c) pengguna juga perlu diberi capaian untuk mengubah maklumat pengesahan(credentials) apabila diperlukan; (d) butiran pengesahan (kata laluan, kunci penyulitan dan token) diperlukan bagi capaian ke sistem maklumat yang mengandungi data sensitif; dan	Pengguna Sistem Pembangun Sistem Pemilik Sistem

5.17 PENGESAHAN MAKLUMAT *(AUTHENTICATION INFORMATION)*	PERANAN
(e) pengendalian maklumat pengesahan yang lemah boleh membawa kepada capaian tanpa kebenaran kepada sistem data dan kehilangan kerahsiaan, ketersediaan dan integriti data sensitif. Perkara yang perlu dipertimbangkan dalam pengurusan dan pentadbiran pengesahan maklumat ; (a) semasa pendaftaran pengguna baharu, penjanaan automatik kata laluan dan nombor identiti persendirian mestilah tidak dapat diteka. Selain itu, setiap pengguna perlu mempunyai kata laluan yang unik dan diwajibkan untuk menukar kata laluan selepas digunakan kali pertama; (b) KKM perlu mempunyai proses yang kukuh untuk menyemak identiti pengguna sebelum diberikan pengesahan identiti yang baharu, penggantian pengesahan identiti atau pengesahan identiti sementara; (c) KKM perlu memastikan keselamatan penghantaran bagi perincian pengesahan kepada individu melalui medium yang selamat dan dilarang dihantar melalui medium elektronik yang tidak selamat (Contoh: plain text); (d) pengguna perlu memastikan mereka menerima perincian pengesahan; dan (e) KKM perlu menyediakan dan memastikan semua rekod berkenaan perkara yang penting berkaitan pengurusan dan pentadbiran pengesahan maklumat disimpan. Perkara ini mestilah dirahsiakan dan cara penyimpanan memerlukan pengesahan hak capaian.	
5.17.2 Peranan dan Tanggungjawab Pengguna Pengguna yang diberikan capaian ke atas maklumat perlu mengikuti amalan terbaik seperti berikut; (a) pengguna perlu memastikan kerahsiaan pengesahan maklumat seperti maklumat kata laluan tidak boleh dipamerkan /dipaparkan / didedahkan secara terbuka atau dikongsi dengan mana-mana pihak; (b) pengguna perlu menukar kata laluan dengan kadar segera jika kerahsiaan kata laluan telah terjejas; (c) pengguna tidak boleh menggunakan kata laluan yang sama untuk perkhidmatan yang lain; dan (d) pengguna perlu memilih kata laluan yang kuat dan sukar untuk diteka dan mematuhi standard keselamatan.	Pengguna Sistem Pembangun Sistem Pemilik Sistem
5.17.3 Pengurusan Kata Laluan Perkara berikut perlu dipatuhi sebagai amalan terbaik dalam pengurusan kata laluan: (a) pengguna perlu mempunyai keupayaan untuk mewujudkan dan mengubah kata laluan, disertakan dengan proses pengesahan untuk mengesan dan membetulkan kesilapan semasa memasukkan data; (b) mematuhi amalan terbaik apabila membangunkan proses pemilihan kata laluan yang terbaik; (c) pengguna perlu menukar kata laluan selepas membuat capaian kali pertama ke dalam sistem;	Pengguna Sistem Pembangun Sistem Pemilik Sistem

5.17 PENGESAHAN MAKLUMAT *(AUTHENTICATION INFORMATION)*	PERANAN
(d) diwajibkan untuk menukar kata laluan apabila diperlukan seperti berikut: (i) selepas berlakunya insiden keselamatan; dan (ii) selepas pegawai berpindah atau meninggalkan tugasnya di mana pegawai tersebut mempunyai capaian menggunakan kata laluan sedia ada. (e) kata laluan terdahulu tidak boleh digunakan kembali; (f) penggunaan kata laluan yang diketahui umum, atau telah digunakan semasa insiden keselamatan tidak boleh digunakan untuk membuat capaian terhadap mana-mana sistem yang telah digodam; (g) apabila kata laluan dimasukkan, kata laluan boleh dipertimbangkan untuk dipaparkan jika diperlukan oleh pengguna; dan (h) kata laluan yang dipindahkan atau disimpan perlu dibuat dalam persekitaran yang selamat; (i) melaksanakan proses *hashing* dan *encryption* berdasarkan cara kriptografi (Bab 8) ke atas maklumat pengesahan; (j) pelaksanaan *Single Sign On* (SSO) juga perlu dipertimbangkan dalam pengurusan log masuk bagi memantau pengurusan sistem dengan lebih berkesan; dan (k) kata laluan perlu mempunyai minima sekurang-kurangnya 12 aksara dengan gabungan alphanumeric dan huruf yang istimewa kecuali bagi peralatan ICT dan perisian yang mempunyai pengurusan kata laluan terhad.	

5.18 HAK CAPAIAN *(ACCESS RIGHTS)*	PERANAN
5.18.1 Peruntukan Capaian Pengguna Proses dan kawalan bagi penugasan, perubahan dan penarikan hak capaian kepada sistem maklumat perlu selari dengan polisi kawalan capaian. Penglibatan pihak ketiga seperti penyelenggaraan atau perkhidmatan secara outsource, sebarang hak capaian yang diberikan hendaklah dikawal dan dipantau selaras dengan keperluan kawalan akses. Pihak ketiga juga bertanggungjawab memaklumkan kepada Pentadbir Sistem, Pembangun Sistem dan Pemilik Sistem mengenai sebarang perubahan berkaitan akses staf mereka. Sistem maklumat atau perkhidmatan perlu diberikan atau dibatalkan berdasarkan perkara berikut; (a) kebenaran daripada pemilik sistem atau perkhidmatan; (b) pengesahan bahawa hak capaian adalah sesuai dengan peranan yang diberikan; dan (c) perlindungan diberikan ke atas hak capaian sebelum kebenaran sebenar diberikan. (d) pengguna perlu diberikan hak capaian setiap masa sepertimana yang tertakluk kepada keperluan perkhidmatan dengan melaksanakan capaian role-based yang berkesan ke atas sistem dan perkhidmatan.	ICTSO Pentadbir Sistem Pembangun Sistem Pemilik Sistem Pihak Ketiga

5.18 HAK CAPAIAN *(ACCESS RIGHTS)*	**PERANAN**
5.18.2 Semakan Hak Capaian Pengguna Pemilik aset perlu menyemak hak capaian pengguna secara berkala sekiranya terdapat perubahan ke atas pegawai (pelantikan, perubahan peranan, dan pemecatan) dan ketika berlakunya semakan audit terhadap kawalan sistem. Kebenaran hak capaian perlu disemak lebih kerap dalam situasi berisiko tinggi yang berkaitan dengan hak capaian istimewa. Perkara ini perlu dilakukan sekurang-kurangnya satu (1) tahun sekali atau pada bila-bila masa ketika perubahan yang ketara dilakukan.	ICTSO Pentadbir Sistem Pembangun Sistem Pemilik Sistem
5.18.3 Pembatalan atau Perubahan Hak Capaian Menjadi perkara penting untuk membatalkan hak capaian ke atas maklumat kepada pegawai dan pihak ketiga semasa penamatan perkhidmatan, kontrak atau perjanjian (atau untuk merubah hak capaian ketika berlakunya perubahan peranan jika perlu). Perkara yang perlu dipertimbangkan dalam pemberian dan pembatalan hak capaian kepada individu adalah seperti berikut; (a) untuk mencapai dan menggunakan aset sistem maklumat berkaitan, pemilik aset sistem maklumat mesti meluluskan penggunaan dan capaian maklumat tersebut. (b) mempertimbangkan kelulusan permohonan hak capaian dengan sekurang-kurangnya dua tahap kelulusan berbeza sebelum hak capaian diberikan; (c) pertimbangan perlu diberikan mengikut keperluan perkhidmatan dan polisi berkenaan kawalan capaian; (d) mempertimbangkan pengagihan tugas. Sebagai contoh, kelulusan dan pelaksanaan hak capaian boleh dilakukan oleh individu berbeza; (e) hak capaian pengguna perlu dibatalkan serta merta apabila tidak lagi diperlukan untuk mencapai aset sistem maklumat, terutama jika pengguna telah meninggalkan KKM; (f) hak capaian sementara boleh diberikan kepada pegawai tetap atau pegawai sementara. Apabila perkhidmatan pegawai telah tamat di KKM, hak capaian perlu dibatalkan; (g) polisi kawalan capaian KKM perlu menentukan tahap capaian individu dan disemak serta disahkan secara berkala. Selain itu, ia perlu mematuhi keperluan keselamatan maklumat yang lain seperti Bab 5; (h) memastikan hak capaian diaktifkan hanya setelah proses kelulusan permohonan hak capaian yang berkaitan telah selesai; (i) hak capaian yang bergantung pada identiti seperti ID atau fizikal perlu diuruskan dalam sistem pengurusan kawalan capaian berpusat (contohnya *Active Directory,LDAP,Single Sign On* dll); (j) mengemas kini tahap hak capaian jika terdapat perubahan tanggungjawab atau peranan; dan (k) kaedah yang boleh digunakan untuk menghapus atau mengubah hak capaian fizikal atau logikal seperti penggantian kunci, kad ID atau maklumat pengesahan	ICTSO Pentadbir Sistem Pembangun Sistem Pemilik Sistem

5.19 KESELAMATAN MAKLUMAT DALAM HUBUNGAN PIHAK KETIGA *(INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS)*	PERANAN
15.19.1 Keselamatan Maklumat dengan Pihak Ketiga Keperluan keselamatan maklumat untuk mengurangkan risiko yang dikaitkan dengan capaian pihak ketiga kepada aset hendaklah dipersetujui dengan pihak ketiga dan didokumenkan. Perkara yang perlu dipertimbangkan adalah seperti berikut: (a) mengekalkan rekod pihak ketiga dengan tepat (Contoh: perkhidmatan kewangan, perkakasan ICT, telefon) yang mempunyai potensi untuk mempengaruhi integriti keselamatan maklumat; (b) memastikan setiap pihak ketiga melaksanakan tapisan keselamatan menerusi sistem yang disediakan oleh CGSO iaitu Sistem e-Vetting; (c) mengenal pasti pihak ketiga yang telah mempunyai capaian sedia ada terhadap kawalan maklumat keselamatan; (d) mengenal pasti dan menentukan kawasan khusus infrastruktur ICT KKM yang mana boleh dicapai, dipantau dan digunakan oleh pihak ketiga; (e) menentukan keupayaan infrastruktur ICT pihak ketiga mematuhi piawaian keselamatan maklumat; (f) mengenal pasti dan menguruskan pelbagai risiko keselamatan maklumat terhadap: (i) pihak ketiga yang menggunakan maklumat sulit atau aset yang dilindungi; (ii) perkakasan pihak ketiga yang rosak atau platform perisian yang tidak berfungsi dengan perkhidmatan awan atau *on-premise*; (g) menghadkan jumlah kerosakan dan/atau gangguan yang berlaku sepanjang ketidakpatuhan. Aktiviti pihak ketiga perlu dipantau dengan cara yang sesuai dan pada tahap yang berbeza-beza berdasarkan tahap risiko. Jika terdapat ketidakpatuhan, sama ada proaktif atau re-aktif, tindakan selanjutnya perlu diambil serta merta; (h) mengekalkan tatacara pengurusan insiden yang cekap bagi mengatasi jumlah kontigensi yang munasabah. (i) menggubal langkah-langkah yang memenuhi ketersediaan dan pemprosesan maklumat pihak ketiga pada bila-bila masa ia digunakan, dengan itu dapat memastikan integriti maklumat KKM terjaga; (j) memahami dan menguruskan tahap risiko yang wujud apabila memindahkan maklumat dan aset fizikal dan maya antara pihak ketiga dan KKM. (k) memastikan hubungan dengan pihak ketiga ditamatkan dengan mengambil kira keselamatan maklumat, termasuk menarik hak capaian dan keupayaan untuk mencapai maklumat; (l) perkara yang perlu dipertimbangkan dalam menarik hak capaian pihak ketiga termasuk: (i) pengagihan harta intelek; (ii) pengalihan maklumat antara pihak ketiga dari/kepada KKM; (iii) pengurusan rekod; (iv) mengembalikan aset ke pemilik asal; (v) pelupusan aset fizikal dan maya termasuk maklumat; dan	Pengurus ICT Pemilik Sistem Pihak Ketiga Pengurus Projek

5.19 KESELAMATAN MAKLUMAT DALAM HUBUNGAN PIHAK KETIGA *(INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS)*	PERANAN
(vi) pematuhan kepada sebarang keperluan kontrak, termasuk klausa kerahsiaan dan/atau perjanjian luar. (m) memastikan pihak ketiga mematuhi dasar, peraturan dan arahan keselamatan KKM yang berkuatkuasa seperti berikut: (i) memastikan pihak ketiga mendapat maklumat berkaitan PKS dan menandatangani Surat Akuan Pematuhan PKS KKM seperti di Lampiran 1; (ii) memastikan pihak ketiga menandatangani Perakuan Akta Rahsia Rasmi 1972 seperti di Lampiran 2; (iii) memastikan pihak ketiga menandatangani Perjanjian Kerahsiaan *(Non-Disclosure Agreement)* seperti di Lampiran 3; (iv) membuat tapisan keselamatan berdasarkan arahan semasa pihak kerajaan; (v) memastikan penamatan perkhidmatan dimaklumkan dan semua keperluan dari pihak kerajaan telah dilaksanakan (Contoh: : mengisi borang,menghapus peranan) (vi) menandatangi Surat Aku Janji; dan (vii) lain-lain peraturan semasa yang sedang berkuatkuasa seperti di Lampiran 4.	
5.20 MENANGANI KESELAMATAN MAKLUMAT DALAM PERJANJIAN PIHAK KETIGA *(ADDRESSING INFORMATION SECURITY WITHIN SUPPLIER AGREEMENTS)*	**PERANAN**
5.20.1 Menangani keselamatan maklumat dalam perjanjian Semua keperluan keselamatan maklumat yang berkaitan hendaklah diwujudkan dan dipersetujui dengan setiap pihak ketiga yang boleh mencapai, memproses, menyimpan, menyampaikan atau menyediakan komponen infrastruktur ICT untuk maklumat KKM. Perkara yang perlu dipatuhi adalah seperti berikut: (a) memberikan penerangan yang jelas tentang maklumat yang perlu dicapai dan bagaimana maklumat itu akan dicapai; (b) KKM perlu mengelaskan maklumat; (c) kedua-dua pihak mesti memahami dengan jelas berkaitan penggunaan maklumat yang boleh diterima dan tidak boleh diterima yang termasuk aset fizikal dan maya; (d) bagi memastikan pihak ketiga boleh mencapai dan melihat maklumat KKM, prosedur perlu dilaksanakan (Contoh: audit pihak ketiga dan kawalan capaian pelayan); (e) perjanjian perlu menerangkan prosedur pengurusan insiden dan bagaimana ia dikendalikan. (f) pihak ketiga perlu disaring sebelum berinteraksi dengan maklumat (Contoh:: e-Vetting CGSO). (g) dasar *BUDR* yang sesuai perlu dilaksanakan oleh pihak ketiga, disesuaikan untuk memenuhi keperluan KKM, yang menguruskan tiga pertimbangan utama: i. jenis sandaran (fail dan folder, tambahan), ii. kekerapan sandaran (harian, mingguan, dsb.)	Pengurus ICT Pemilik Sistem Pihak Ketiga Pengurus Projek

5.20 MENANGANI KESELAMATAN MAKLUMAT DALAM PERJANJIAN PIHAK KETIGA *(ADDRESSING INFORMATION SECURITY WITHIN SUPPLIER AGREEMENTS)*	PERANAN
iii. lokasi sandaran dan media sumber (di tapak, luar tapak). (h) pihak ketiga perlu mengekalkan dasar pengurusan perubahan yang komprehensif yang membolehkan KKM menolak sebarang perubahan yang mungkin menjejaskan keselamatan maklumat; (i) kawalan keselamatan fizikal perlu dilaksanakan bergantung pada maklumat yang dibenarkan untuk dicapai (capaian bangunan, capaian pelawat, capaian bilik, keselamatan meja); (j) apabila data dipindahkan antara aset, tapak, pelayan atau lokasi storan, pihak ketiga hendaklah memastikan data dan aset dilindungi daripada kehilangan, kerosakan atau pencemaran; (k) sebagai sebahagian daripada perjanjian, setiap pihak hendaklah dikehendaki mengambil tindakan sekiranya berlaku penamatan (lihat Bab 5). Tindakan ini termasuk (tetapi tidak terhad kepada): i. melupuskan aset dan/atau penempatan semula; ii. menghapus maklumat; iii. mengembalikan IP; iv. mengalih keluar hak capaian; dan v. meneruskan kewajipan kerahsiaan. (l) sebagai tambahan pihak ketiga perlu membincangkan secara terperinci bagaimana ia berhasrat untuk menghapuskan maklumat KKM secara kekal apabila ia tidak diperlukan lagi (iaitu selepas penamatan kontrak); dan (m) apabila kontrak tamat dan terdapat keperluan untuk memindahkan sokongan dan/atau perkhidmatan kepada pihak ketiga lain yang tidak disenaraikan dalam kontrak, langkah-langkah perlu diambil untuk memastikan tiada gangguan kepada operasi perkhidmatan.	
5.21 MENGURUS KESELAMATAN MAKLUMAT DALAM RANTAIAN BEKALAN ICT *(MANAGING INFORMATION SECURITY IN THE ICT SUPPLY CHAIN)*	**PERANAN**
5.21.1 Rantaian Bekalan Teknologi Maklumat dan ICT Perjanjian dengan pihak ketiga hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Beberapa kawalan bagi menangani hubungan dengan pihak ketiga dan kewajipan pihak ketiga dengan sub kontraktor pada bahagian rantaian bekalan kepada pihak yang lain. Perkara yang perlu diambil kira seperti berikut: (a) menentukan keperluan keselamatan maklumat yang komprehensif dan jelas jelas tentang bagaimana pihak ketiga perlu bertindak dalam menyediakan produk dan perkhidmatan ICT; (b) pihak ketiga bertanggungjawab untuk memastikan kontraktor dan pegawai mereka memahami sepenuhnya piawaian keselamatan maklumat di KKM ini. Perkara ini perlu sekiranya mereka melantik pihak yang lain dari mana-mana elemen rantaian bekalan; (c) pihak ketiga mesti menyampaikan keperluan keselamatan KKM ini	Pengurus Projek

5.20 MENANGANI KESELAMATAN MAKLUMAT DALAM PERJANJIAN PIHAK KETIGA *(ADDRESSING INFORMATION SECURITY WITHIN SUPPLIER AGREEMENTS)*	PERANAN
kepada mana-mana pembekal atau pihak lain yang mereka gunakan apabila timbul keperluan untuk memperoleh komponen (fizikal atau maya) daripada pihak yang lain; (d) KKM perlu meminta maklumat daripada pihak ketiga mengenai sifat dan fungsi komponen perisian; (e) KKM perlu mengenal pasti dan mengendalikan sebarang produk atau perkhidmatan yang disediakan dengan cara yang tidak menjejaskan keselamatan maklumat; (f) sebarang produk atau perkhidmatan yang dihantar oleh pihak ketiga perlu dipastikan selamat dan mematuhi piawaian industri. Beberapa kaedah boleh digunakan untuk memastikan pematuhan, termasuk pemeriksaan pensijilan, ujian dalaman dan dokumentasi sokongan; (g) sebagai sebahagian daripada penerimaan produk atau perkhidmatan, KKM perlu mengenal pasti dan merekodkan sebarang elemen yang dianggap penting untuk mengekalkan fungsi teras – terutamanya jika komponen tersebut diperoleh daripada sub kontraktor atau perjanjian penyumberan luar; (h) pihak ketiga perlu memberi jaminan bahawa "komponen kritikal" dapat dijejaki sepanjang rantaian bekalan ICT dari mula hingga penghantaran sebagai sebahagian daripada log audit; (i) KKM perlu mendapatkan jaminan sebelum menyampaikan produk dan perkhidmatan ICT. Ini adalah untuk memastikan ia beroperasi mengikut spesifikasi dan tidak mengandungi sebarang ciri tambahan yang mungkin menimbulkan risiko keselamatan; (j) spesifikasi komponen adalah penting untuk memastikan KKM memahami komponen perkakasan dan perisian yang diperkenalkan kepada rangkaiannya; (k) penting untuk mendapatkan jaminan mengenai pematuhan produk ICT dengan standard industri dan keperluan keselamatan khusus sektor mengikut keperluan khusus produk. Pihak ketiga perlu memperoleh tahap minimum pensijilan keselamatan formal atau mematuhi satu set piawaian maklumat yang diiktiraf di peringkat antarabangsa; dan (l) prosedur perlu diwujudkan untuk mengurus risiko apabila beroperasi dengan komponen yang tidak disokong atau usang di mana sahaja ia berada.	
5.22 PEMANTAUAN , PENILAIAN DAN PENGURUSAN PERUBAHAN PERKHIDMATAN PIHAK KETIGA *(MONITORING, REVIEW AND CHANGE MANAGEMENT OF SUPPLIER SERVICES)*	**PERANAN**
5.22.1 Memantau dan Mengkaji Semula Perkhidmatan Pembekal KKM perlu sentiasa memantau, mengkaji semula, mengaudit perkhidmatan pembekal secara berkala dan mengurus perubahan dalam amalan risiko keselamatan maklumat pembekal dan penyampaian perkhidmatan. KKM perlu memastikan bahawa pegawai bertanggungjawab untuk menguruskan SLA dan hubungan dengan pihak ketiga yang mempunyai kepakaran dalam bidang tertentu dan sumber teknikal. Perkara ini perlu bagi memastikan mereka mampu menilai prestasi pihak ketiga sebaiknya dan tiada pelanggaran piawaian keselamatan maklumat.	Pengurus Projek Pihak ketiga Pemilik Sistem

5.22 PEMANTAUAN , PENILAIAN DAN PENGURUSAN PERUBAHAN PERKHIDMATAN PIHAK KETIGA *(MONITORING, REVIEW AND CHANGE MANAGEMENT OF SUPPLIER SERVICES)*	**PERANAN**
Perkara yang perlu diambil kira adalah seperti berikut: (a) memastikan perubahan dalam perkhidmatan Pihak Ketiga dipersetujui bersama dan menguntungkan pihak kerajaan; (b) pemantauan berterusan tahap perkhidmatan berdasarkan SLA yang ditetapkan, dan menangani sebarang kelemahan apabila ia terjadi. (c) sebarang perubahan kepada perkhidmatan termasuk namun tidak terhad kepada; (i) perubahan infrastruktur; (ii) pemasangan teknologi baharu; (iii) kemaskini produk dan naik taraf versi; (iv) perubahan kepada persekitaran pembangunan; (v) perubahan logistik dan fizikal terhadap fasiliti pihak ketiga, termasuk lokasi baharu. (vi) perubahan terhadap rakan kongsi sumber luar atau sub kontraktor; dan (vii) maklumat kritikal KKM, sistem serta proses yang terlibat dan kajian risiko. (d) memastikan laporan perkhidmatan dilaksanakan dengan berkala, data yang diperoleh dianalisis dan mesyuarat semakan dijalankan berdasarkan SLA; (e) menjalankan semakan insiden keselamatan berdasarkan kaedah yang dipersetujui dengan pihak ketiga dan berdasarkan garis panduan, arahan, polisi yang berkait dengan pengurusan insiden; (f) rekod perlu diselenggara bagi semua insiden keselamatan maklumat, masalah operasi, log rosak dan had asas bagi memenuhi piawaian penyampaian perkhidmatan; (g) mengambil langkah proaktif terhadap insiden berkaitan keselamatan maklumat; (h) mengenal pasti sebarang kerentanan dalam keselamatan maklumat dan melaksana pencegahan; (i) melakukan analisa terhadap faktor keselamatan maklumat yang berkaitan melibatkan pihak ketiga dengan pihak lain dan sub kontraktor; dan (j) memastikan pihak ketiga mengekalkan piawaian asas untuk keselamatan maklumat secara berkala.	
5.23 KESELAMATAN MAKLUMAT UNTUK PENGGUNAAN PERKHIDMATAN AWAN *(INFORMATION SECURITY FOR USE OF CLOUD SERVICES)*	**PERANAN**
5.23.1 Keselamatan maklumat Untuk Perkhidmatan Awan Proses untuk perolehan, penggunaan, pengurusan dan pembatalan daripada perkhidmatan awan hendaklah menggunakan arahan, polisi, peraturan yang sedang berkuatkuasa. Pematuhan kepada kawalan ini adalah sebagai usaha kerjasama antara KKM dan rakan kongsi perkhidmatan awan. Kawalan ini juga perlu diselaras bagi pengurusan maklumat dalam rantaian bekalan dan pengurusan perkhidmatan pihak ketiga.	Pentadbir Sistem Pentadbir Pengkomputeran Awan

5.23 KESELAMATAN MAKLUMAT UNTUK PENGGUNAAN PERKHIDMATAN AWAN *(INFORMATION SECURITY FOR USE OF CLOUD SERVICES)*	**PERANAN**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) memastikan kepatuhan terhadap keperluan perundangan, peraturan, panduan dan perjanjian kontrak yang berkaitan antaranya: (i) PK 2.6: Perolehan Perkhidmatan Pengkomputeran Awan (Cloud) Sektor Awam; (ii) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021 Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam; dan (iii) Surat Pekeliling Am Bilangan 2 Tahun 2021 Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan. (b) menentukan/mentakrifkan dan memaklumkan cara/kaedah berkaitan pengurusan risiko bagi perkhidmatan pengkomputeran awan; (c) memastikan keperluan keselamatan maklumat yang berkaitan dengan penggunaan perkhidmatan pengkomputeran awan dilaksanakan; (d) melaksanakan kawalan terhadap keperluan pelesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan; (e) capaian kepada mana-mana platform awan memenuhi sempadan keperluan keselamatan maklumat KKM; (f) pertimbangan yang mencukupi diberikan kepada perkhidmatan antimalware dan antivirus, termasuk pemantauan proaktif dan perlindungan ancaman; (g) pembekal awan mematuhi set storan dan pemprosesan data yang telah ditetapkan, yang berkaitan dengan peraturan kawal selia terhadap satu atau lebih kawasan global;	

5.23 KESELAMATAN MAKLUMAT UNTUK PENGGUNAAN PERKHIDMATAN AWAN *(INFORMATION SECURITY FOR USE OF CLOUD SERVICES)*	**PERANAN**
5.23.1 Keselamatan maklumat Untuk Perkhidmatan Awan Proses untuk perolehan, penggunaan, pengurusan dan pembatalan daripada perkhidmatan awan hendaklah menggunakan arahan, polisi, peraturan yang sedang berkuatkuasa. Pematuhan kepada kawalan ini adalah sebagai usaha kerjasama antara KKM dan rakan kongsi perkhidmatan awan. Kawalan ini juga perlu diselaras bagi pengurusan maklumat dalam rantaian bekalan dan pengurusan perkhidmatan pihak ketiga. Perkara yang perlu dipatuhi adalah seperti berikut: (a) memastikan kepatuhan terhadap keperluan perundangan, peraturan, panduan dan perjanjian kontrak yang berkaitan antaranya: (i) PK 2.6: Perolehan Perkhidmatan Pengkomputeran Awan (Cloud) Sektor Awam; (ii) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021 Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam; dan (iii) Surat Pekeliling Am Bilangan 2 Tahun 2021 Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan.	Pentadbir Sistem Pentadbir Pengkomputeran Awan

5.23 KESELAMATAN MAKLUMAT UNTUK PENGGUNAAN PERKHIDMATAN AWAN *(INFORMATION SECURITY FOR USE OF CLOUD SERVICES)*	PERANAN
(b) menentukan/mentakrifkan dan memaklumkan cara/kaedah berkaitan pengurusan risiko bagi perkhidmatan pengkomputeran awan; (c) memastikan keperluan keselamatan maklumat yang berkaitan dengan penggunaan perkhidmatan pengkomputeran awan dilaksanakan; (d) melaksanakan kawalan terhadap keperluan pelesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan; (e) capaian kepada mana-mana platform awan memenuhi sempadan keperluan keselamatan maklumat KKM; (f) pertimbangan yang mencukupi diberikan kepada perkhidmatan antimalware dan antivirus, termasuk pemantauan proaktif dan perlindungan ancaman; (g) pembekal awan mematuhi set storan dan pemprosesan data yang telah ditetapkan, yang berkaitan dengan peraturan kawal selia terhadap satu atau lebih kawasan global; (h) sokongan proaktif diberikan kepada KKM, sekiranya platform awan mengalami kegagalan besar atau insiden berkaitan keselamatan maklumat; (i) jika timbul keperluan untuk membuat subkontrak atau sebaliknya menyumber luar mana-mana elemen platform awan, keperluan keselamatan maklumat pihak ketiga kekal sebagai pertimbangan berterusan; (j) sekiranya KKM memerlukan sebarang bantuan dalam mengumpul maklumat digital untuk sebarang tujuan yang berkaitan (penguatkuasaan undang-undang, penjajaran kawal selia,), penyedia perkhidmatan awan akan memberi bantuan penuh; (k) pembekal perkhidmatan awan perlu memberikan sokongan yang munasabah dan ketersediaan yang sesuai semasa tempoh peralihan atau penyahtauliahan; (l) pembekal perkhidmatan awan beroperasi dengan pelan BUDR yang mantap yang menumpukan pada pelaksanaan sandaran data KKM yang mencukupi; dan (m) pemindahan semua data tambahan yang berkaitan daripada penyedia perkhidmatan awan kepada KKM, termasuk maklumat konfigurasi dan kod yang dituntut oleh KKM.	
5.24 PERANCANGAN DAN PENYEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY INCIDENT MANAGEMENT PLANNING AND PREPARATION)*	**PERANAN**
5.24.1 Perancangan dan Persediaan Tanggungjawab dan prosedur pengurusan insiden keselamatan maklumat hendaklah disediakan bagi memastikan tindak balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan insiden KKM adalah berdasarkan kepada polisi, arahan, garis panduan dan lain-lain peraturan yang sedang berkuatkuasa.	ICTSO Pengurus ICT Penyelaras ICT Fasiliti CSIRT IPKKM CSIRT Fasiliti KKM

5.24 PERANCANGAN DAN PENYEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY INCIDENT MANAGEMENT PLANNING AND PREPARATION)*	**PERANAN**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) melaksana pengendalian insiden keselamatan siber dengan merujuk kepada garis polisi, arahan, garis panduan dan lain-lain peraturan yang sedang berkuatkuasa (b) mempertimbangkan keperluan untuk belajar daripada insiden apabila ia telah diselesaikan. Ini menghalang pengulangan dan menyediakan pegawai dengan konteks sejarah untuk senario masa depan; (c) memastikan hanya pegawai terlatih dan cekap terlibat dalam pengurusan dan pengendalian insiden. Di samping itu, pastikan mereka mempunyai capaian penuh kepada dokumentasi prosedur dan diberikan latihan terkini yang berkaitan secara langsung dengan insiden keselamatan maklumat; dan (d) mengenal pasti keperluan latihan dan pensijilan pegawai dalam menyelesaikan insiden berkaitan keselamatan maklumat.	
5.25 PENILAIAN DAN KEPUTUSAN MENGENAI INSIDEN KESELAMATAN MAKLUMAT *(ASSESSMENT AND DECISION ON INFORMATION SECURITY EVENTS)*	**PERANAN**
5.25.1 Penilaian Keputusan Mengenai Insiden Keselamatan Maklumat Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat berdasarkan pekeliling dan prosedur pengurusan insiden keselamatan maklumat yang sedang berkuat kuasa. Penilaian ini hendaklah dilakukan mengikut panduan seperti berikut: **(a) Pengkategorian Peristiwa dan Insiden** Untuk membezakan insiden keselamatan maklumat daripada peristiwa keselamatan maklumat, KKM perlu bekerjasama untuk bersetuju terhadap sistem pengkategorian; **(b) Libat Urus Pegawai Teknikal** Pegawai teknikal yang mempunyai kemahiran berkaitan serta akses kepada alat pemantauan dan analisis perlu dilibatkan bagi membantu dalam mengenal pasti, menganalisis dan mengurus insiden. **(c) Keputusan Secara Konsensus** Keputusan sama ada sesuatu peristiwa perlu diisytiharkan sebagai insiden keselamatan maklumat hendaklah dibuat secara bersama oleh semua pihak yang berkaitan. **(d) Rekod Penilaian dan Keputusan** Semua aktiviti berkaitan termasuk perbincangan, penilaian dan keputusan pengkategorian hendaklah direkodkan dengan teratur untuk tujuan pelaporan, rujukan masa hadapan dan penambahbaikan proses pengurusan insiden.	ICTSO Pengurus ICT CSIRT IPKKM CSIRT Fasiliti KKM

5.26 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT *(RESPONSE TO INFORMATION SECURITY INCIDENTS)*	**PERANAN**
5.26.1 Tindak Balas Terhadap Insiden Tindak balas Insiden keselamatan maklumat hendaklah dikendalikan berdasarkan kepada polisi, arahan, garis panduan dan lain-lain peraturan yang sedang berkuatkuasa. Untuk memastikan penyelesaian segera dan menyeluruh bagi sebarang insiden keselamatan maklumat, CSIRT telah ditubuhkan bagi mengendali setiap insiden Perkara yang perlu dipatuhi dalam tindak balas insiden adalah seperti berikut: (a) bukti perlu dikumpul dan disokong sejurus selepas insiden keselamatan maklumat; (b) merancang langkah seterusnya, termasuk pengurusan krisis dan kesinambungan perkhidmatan (lihat Bab 5); (c) analisa post-mortem memerlukan rekod log yang tepat dari semua aktiviti berkenaan insiden termasuk tindakan awal/pertama; (d) penyampaian maklumat keselamatan berkaitan insiden perlu disalurkan berdasarkan peraturan yang berkuat kuasa; (e) mengambil kira tanggungjawab KKM terhadap organisasi luar (pelanggan, vendor, badan awam, pengawal selia, dll.) apabila membincangkan kesan yang lebih luas daripada insiden keselamatan maklumat; (f) analisis forensik dilakukan ke atas insiden; (g) sebaik sahaja insiden telah diselesaikan, punca asas perlu dikenal pasti, direkodkan dan dimaklumkan kepada semua pihak yang berkaitan (lihat Bab 5); dan (h) menangani kelemahan asas yang membawa kepada insiden dan peristiwa yang berkaitan dengan keselamatan maklumat, termasuk pengenalpastian dan pengubahsuaian proses dalaman, kawalan, dasar dan prosedur.	ICTSO Pengurus ICT CSIRT IPKKM CSIRT Fasiliti KKM
5.27 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT *(LEARNING FROM INFORMATION SECURITY INCIDENTS)*	**PERANAN**
5.27.1 Pembelajaran dari Insiden Keselamatan Maklumat Pengetahuan yang diperoleh daripada insiden keselamatan maklumat perlu digunakan untuk memperkuatkan dan meningkatkan kawalan keselamatan maklumat serta digunakan bagi mengurangkan risiko kejadian berulang. Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambahbaik. Setelah semakan dan pembelajaran selesai, kemas kini kepada polisi, arahan, peraturan perlu dibuat dan pegawai yang berkaitan dimaklumkan dan dilatih untuk memastikan kitaran kesedaran dan pendidikan keselamatan maklumat diteruskan. KKM perlu melaksanakan dasar pengurusan insiden yang mengkategorikan dan memantau tiga elemen utama insiden keselamatan maklumat di seluruh operasi mereka iaitu:	ICTSO Pengurus ICT CSIRT IPKKM CSIRT Fasiliti KKM

5.27 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT *(LEARNING FROM INFORMATION SECURITY INCIDENTS)*	**PERANAN**
(a) Jenis *(Type)* (b) Jumlah *(Volume)* (c) Kos *(Cos)t* Selepas insiden telah ditutup, ia perlu dianalisis dengan teliti untuk penambahbaikan prosedur sedia ada. Antara tindakan yang perlu diambil selepas insiden adalah seperti berikut: (a) membangunkan rangka kerja pengurusan insiden menyeluruh yang merangkumi unjuran senario dan prosedur yang berkaitan (lihat Bab 5). (b) meningkatkan daya tahan semua kategori insiden dengan menambah baik proses dan prosedur penilaian risiko keselamatan maklumat KKM. (c) meningkatkan kesedaran pengguna dengan membincangkan cara bertindak balas, mengelak dan menyelesaikan insiden lalu.	
5.28 PENGUMPULAN BUKTI *(COLLECTION OF EVIDENCE)*	**PERANAN**
5.28.1 Pengumpulan Bahan Bukti Insiden KKM hendaklah menentukan dan menggunakan prosedur untuk mengenal pasti, mengumpul, memperoleh dan memelihara maklumat yang boleh digunakan sebagai bukti. Adalah penting untuk mengumpul bukti tepat pada masanya kerana ia memberikan maklumat berkaitan insiden bagi keperluan pematuhan ke atas prosiding undang-undang. Pengumpulan bukti perlu mengambil kira perkara-perkara berikut: (a) rantaian penjaga (chain of custody) yang berkaitan; (b) keselamatan bukti; (c) keselamatan personel; (d) peranan dan tanggungjawab personel yang terlibat; (e) kompetensi personel; (f) dokumentasi; dan (g) taklimat berkaitan pengumpulan bukti.	ICTSO Pengurus ICT CSIRT IPKKM CSIRT Fasiliti KKM
5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN *(INFORMATION SECURITY DURING DISRUPTION)*	**PERANAN**
5.29.1 Keselamatan Maklumat Semasa Gangguan Keselamatan maklumat perlu menjadi bahagian penting dalam pelan pengurusan kesinambungan perkhidmatan KKM. KKM perlu membuat rancangan untuk mengekalkan keselamatan maklumat dan memulihkannya jika sebarang gangguan operasi atau kegagalan sistem membawa kepada insiden keselamatan. Tahap keselamatan mesti dikembalikan ke tahap pra-gangguan dengan cara yang cepat, untuk mengelakkan sebarang bahaya yang lain. Aspek penting berkaitan dengan keselamatan maklumat semasa gangguan yang perlu diberi perhatian ialah seperti yang berikut: (a) pembangunan dan pelaksanaan Pelan Perancangan Kesinambungan Perkhidmatan (Business Continuity Planning) untuk memastikan	CDO ICTSO Pengurus ICT CSIRT IPKKM CSIRT Fasiliti KKM Pasukan PKP

5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN *(INFORMATION SECURITY DURING DISRUPTION)*	PERANAN
penyampaian perkhidmatan berfungsi dengan minimum gangguan ketika terjadi insiden; (b) pemulihan Bencana melibatkan pelan dan tindakan untuk memulihkan sistem maklumat dan data setelah bencana atau insiden; (c) perlindungan Data melibatkan Salinan data secara berkala, pengekalan data yang baik, dan pelaksanaan tindakan keselamatan yang sesuai untuk melindungi data terperingkat; (d) pencegahan Serangan Siber (Cybersecurity Measures) melibatkan tindakan untuk mencegah serangan siber dan melindungi data daripada ancaman siber; (e) pemulihan Sistem Pantas (Quick System Recovery) untuk mengurangkan masa henti ketika terjadi gangguan; (f) kawalan fizikal ke pusat data dan peralatan komputer terhad kepada individu yang sah untuk mencegah capaian yang tidak dibenarkan; (g) pemulihan data memastikan keupayaan untuk memulihkan data yang hilang atau terjejas dalam insiden; (h) kesedaran keselamatan (Security Awareness) untuk mengurangkan ancaman dalaman dan mencegah insiden yang disebabkan oleh kesilapan manusia; (i) Pelan Komunikasi Krisis (Crisis Communication Plan) yang jelas untuk mengurus krisis dan insiden dengan pantas.	CDO ICTSO Pengurus ICT CSIRT IPKKM CSIRT Fasiliti KKM Pasukan PKP
5.30 KESEDIAAN ICT UNTUK KESINAMBUNGAN PERKHIDMATAN *(ICT READINESS FOR BUSINESS CONTINUITY)*	**PERANAN**
5.30.1 Kesediaan ICT Kesediaan ICT perlu dirancang, dilaksanakan, dikekalkan, dan diuji berdasarkan objektif kesinambungan perkhidmatan dan keperluan kesinambungan ICT. Kesinambungan keselamatan maklumat hendaklah diterapkan ke dalam sistem pengurusan kesinambungan bisnes KKM.	CDO Pengurus ICT Penyelaras ICT Fasiliti Pasukan PKP Pegawai Kejuruteraan
5.30.2 Perancangan Kesinambungan Perkhidmatan KKM hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, KKM perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi KKM. KKM juga perlu mengambil kira keperluan dan harapan pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: (a) melantik pasukan tadbir urus Pelan Kesinambungan Perkhidmatan (PKP) ; (b) menetapkan polisi PKP; (c) mengenal pasti perkhidmatan kritikal; (d) melaksanakan Kajian Impak Perkhidmatan (Business Impact Analysis,BIA) dan Penilaian Risiko terhadap perkhidmatan kritikal; (e) membangunkan Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT;	CDO Pengurus ICT Penyelaras ICT Fasiliti Pasukan PKP Pegawai Kejuruteraan

5.30 KESEDIAAN ICT UNTUK KESINAMBUNGAN PERKHIDMATAN *(ICT READINESS FOR BUSINESS CONTINUITY)*	PERANAN
(f) melaksanakan program kesedaran dan latihan pasukan PKP dan pegawai; melaksanakan simulasi pelan kesinambungan perkhidmatan; dan (g) melaksana penyelenggaraan ke atas pelan kesinambungan perkhidmatan.	
5.30.3 Pelaksanaan Kesinambungan Keselamatan Maklumat KKM hendaklah menyedia, mendokumentasi, melaksana dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan ialah seperti yang berikut: (a) melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal KKM yang telah dikenal pasti berdasarkan kepada Pelan Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak Balas Kecemasan dan Pelan Pemulihan Bencana; (b) melaksanakan pasca nilai (post-mortem) dan mengemas kini pelan-pelan yang terlibat; (c) mengemas kini pelan-pelan yang terlibat jika berlaku perubahan kepada fungsi kritikal KKM; (d) mengemas kini struktur tadbir urus PKP KKM sekiranya berlaku pertukaran keahlian pasukan; dan (e) memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP.	CDO Pengurus ICT Penyelaras ICT Fasiliti Pasukan PKP Pegawai Kejuruteraan
5.30.4 Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat KKM hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan sekurang-kurangnya setahun sekali bagi memastikannya terpakai dan berkesan semasa situasi kecemasan. Kesediaan ICT hendaklah dirancang, dilaksanakan, diselenggara dan diuji berdasarkan objektif kesinambungan perkhidmatan dan keperluan kesinambungan ICT. KKM hendaklah memastikan bahawa: (a) struktur pasukan PKP yang mencukupi disediakan untuk bertindak balas terhadap gangguan; (b) pelan PKP dan pelan-pelan lain yang terlibat termasuk tindak balas dan prosedur pemulihan hendaklah dinilai dan diuji melalui pelaksanaan simulasi sekurang-kurangnya setahun sekali serta diluluskan oleh pihak pengurusan; (c) pelan PKP hendaklah mengandungi perkara seperti yang berikut: (i) spesifikasi prestasi dan kapasiti untuk memenuhi keperluan dan objektif kesinambungan perkhidmatan seperti yang dinyatakan dalam Business Impact Analysis (BIA); (ii) ***Recovery Time Objective*** (RTO) bagi setiap perkhidmatan ICT mengikut keutamaan pemulihan dan prosedur untuk memulihkan komponen tersebut; dan (iii) ***Recovery Point Objective*** (RPO) bagi setiap perkhidmatan ICT mengikut keutamaan pemulihan dan prosedur untuk memulihkan komponen tersebut.	CDO Pengurus ICT Penyelaras ICT Fasiliti Pasukan PKP Pegawai Kejuruteraan

5.31 UNDANG-UNDANG, BERKANUN, PERATURAN DAN KEPERLUAN KONTRAK *(LEGAL, STATUTORY, REGULATORY AND CONTRACTUAL REQUIREMENTS)*	PERANAN
5.31.1 Pematuhan Terhadap Keperluan Perundangan dan Kontrak Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh pegawai KKM, pihak ketiga dan pihak yang mempunyai urusan dengan perkhidmatan di KKM. KKM perlu memahami tanggungjawab pada setiap masa, dan bersedia untuk mengubah suai langkah keselamatan maklumat agar sesuai dengan peranan sebagai pengendali data yang boleh dipercayai. Senarai keperluan perundangan dan peraturan-peraturan yang perlu dipatuhi oleh semua pengguna dan pihak ketiga seperti di Lampiran 4. KKM mesti mengingati kewajipan undang-undang, berkanun, peraturan dan kontrak apabila: (a) menggubal atau meminda prosedur keselamatan maklumat dan polisi dalaman mereka; (b) mereka bentuk, mengubah dan melaksanakan kawalan keselamatan maklumat; (c) ketika menilai keperluan keselamatan data secara meluas, kedua-dua jabatan atau apa-apa berkaitan pihak ketiga, mesti mengkategorikan keselamatan maklumat mereka; (d) menjalankan penilaian risiko yang berkaitan dengan aktiviti keselamatan data, seperti peranan dalaman dan struktur KKM; dan (e) menentukan hubungan dengan pihak ketiga, serta kewajipan kontrak sepanjang perkhidmatan bekalan.	CDO Pengurus ICT Penyelaras ICT Fasiliti
5.31.2 Perundangan dan Peraturan KKM perlu menggariskan dan merekodkan prosedur dan peranan dalaman dengan jelas supaya: (a) mengenal pasti, menganalisa dan memahami keperluan undang-undang dan peraturan berkenaan keselamatan maklumat, termasuk penilaian undang-undang dan peraturan yang konsisten. (b) memastikan mereka terus mematuhi semua keperluan undang-undang dan peraturan di setiap negara tempat mereka beroperasi, serta sebarang produk dan perkhidmatan dari luar negara.	CDO Pengurus ICT Penyelaras ICT Fasiliti
5.31.3 Panduan Kriptografi Kriptografi ialah teknik untuk melindungi maklumat dan komunikasi dengan menggunakan teknik pengekodan. Perkara ini dapat memastikan maklumat tersebut selamat seterusnya menjamin komunikasi antara dua pihak. Penggunaan penyulitan dan kriptografi memerlukan pematuhan peraturan undang-undang yang ditetapkan dan beberapa nasihat pengawalseliaan yang berkaitan Penggunaan kriptografi hendaklah mematuhi keperluan perundangan, dasar dan pekeliling seperti yang berikut: (i) Akta Kerajaan Elektronik 2007; (ii) Akta Tandatangan Digital 1997; (iii) Dasar Kriptografi Negara; dan (iv) Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bilangan 3 Tahun 2015 Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastructure (GPKI)]	CDO Pengurus ICT Penyelaras ICT Fasiliti

5.32 HAK HARTA INTELEK *(INTELLECTUAL PROPERTY RIGHTS)*	PERANAN
5.32.1 Hak Harta Intelek KKM perlu memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Semua pihak yang terlibat hendaklah melaksanakan kawalan terhadap keperluan pelesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	Pengurus ICT Pemilik Sistem Penyelaras ICT Fasiliti Pihak Ketiga Pegawai KKM Pemilik Sistem
5.33 PERLINDUNGAN REKOD *(PROTECTION OF RECORDS)*	**PERANAN**
KKM hendaklah memastikan pengurusan rekod dilaksanakan secara teratur, selamat dan mematuhi undang-undang serta keperluan organisasi. Proses ini merangkumi pengekalan, pengendalian, penyimpanan, pelupusan dan pemulihan rekod, termasuk rekod elektronik, bagi menjamin integriti, kerahsiaan, kebolehcapaian serta pematuhan kepada keperluan undang-undang dan piawaian. Lima risiko utama dalam perlindungan rekod; (a) pemalsuan; (b) akses tanpa kebenaran; (c) keluaran atau penerbitan tanpa kebenaran; (d) kehilangan; dan (e) kemusnahan. Berdasarkan kawalan ini, KKM hendaklah: (a) merujuk garis panduan yang berkuatkuasa terhadap empat fungsi utama serta topik khusus berkaitan rekod, iaitu: i. pelupusan rekod; ii. pencegahan manipulasi rekod; iii. penyimpanan rekod; iv. rantaian jagaan dalam pengendalian rekod; (b) mengekalkan jadual penyimpanan rekod yang menetapkan tempoh simpanan bagi setiap jenis rekod, selaras dengan tujuan perkhidmatan masing-masing; (c) membangunkan proses penyimpanan dan pengendalian rekod dengan mengambil kira perkara berikut: i. pematuhan kepada undang-undang atau peraturan berkaitan penyimpanan rekod yang berkuat kuasa; ii. jangkaan komuniti dan orang awam terhadap cara KKM mengurus rekod mereka; (d) memusnahkan rekod dengan cara yang selamat dan sesuai sebaik sahaja tempoh pengekalan rekod tamat; (e) mengkategorikan rekod mengikut tahap risiko keselamatan, tempoh pengekalan dan media simpanan, termasuk tetapi tidak terhad kepada: i. rekod peribadi; ii. rekod undang-undang; iii. rekod perakaunan; iv. rekod transaksi perkhidmatan;	Pengurus ICT Penyelaras ICT Fasiliti Pemilik Aset Pihak Ketiga Pegawai KKM Pemilik Sistem

5.33 PERLINDUNGAN REKOD *(PROTECTION OF RECORDS)*	PERANAN
(f) memastikan prosedur penyimpanan membolehkan rekod diperoleh semula dalam tempoh masa yang munasabah apabila diminta oleh pihak ketiga atau secara dalaman; (g) bagi rekod elektronik, mempertimbangkan dan mengurangkan risiko halangan capaian semasa pemulihan akibat perubahan teknologi, contohnya dengan menyimpan butiran kriptografi yang berkaitan; dan (h) mematuhi arahan pengilang dalam penyimpanan dan pengurusan rekod elektronik, serta mengambil kira risiko kemerosotan semula jadi media simpanan.	
5.34 PRIVASI DAN PERLINDUNGAN DATA PERIBADI *(PRIVACY AND PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION)*	**PERANAN**
5.34.1 Privasi dan Perlindungan Data Peribadi Maklumat peribadi merujuk kepada sebarang data yang boleh digunakan untuk mengenal pasti individu seperti nombor kad pengenalan, rekod perubatan dan lain-lain. Jika terdapat sebarang keperluan terhadap pengenalan tersebut hendaklah terlebih dahulu mendapat persetujuan daripada individu berkenaan. Pelaksanaan perlindungan maklumat peribadi di KKM adalah selaras dengan peruntukan yang dinyatakan dalam Akta Perlindungan Data Peribadi yang terkini.	CDO Pengurus ICT Penyelaras ICT Fasiliti ICTSO IPKKM ICTSO Fasiliti Pihak Ketiga Pegawai KKM Pemilik Sistem
5.35 KAJIAN SEMULA KESELAMATAN MAKLUMAT SECARA BERKECUALI *(INDEPENDENT REVIEW OF INFORMATION SECURITY)*	**PERANAN**
5.35.1 Kajian Semula Keselamatan Maklumat Secara Berkecuali Penilaian keselamatan maklumat oleh pihak ketiga pada masa yang dirancang atau apabila berlaku perubahan operasi yang besar perlu dilaksanakan oleh KKM. Ia penting bagi menjamin pengurusan keselamatan maklumat sentiasa relevan dan berkecuali. Kawalan ini memastikan bahawa KKM: (a) mempunyai keupayaan untuk memenuhi keperluan dan mencukupi; (b) mencapai objektif yang betul; dan (c) mempunyai prestasi yang berkesan supaya berfungsi seperti yang direka. KKM perlu merangka dan melaksanakan prosedur yang membenarkan kajian berasingan terhadap amalan keselamatan maklumat. Kajian semula perlu memberi tumpuan kepada mengenal pasti bidang untuk penambahbaikan dalam pendekatan KKM terhadap keselamatan maklumat, termasuk: (a) polisi keselamatan maklumat; (b) dasar yang disesuaikan dengan topik tertentu; dan (c) kawalan berkaitan. Penemuan semakan hendaklah direkodkan dengan teliti, disimpan bagi tujuan pelaporan kepada pihak yang berkepentingan. Semakan berkala atau ad hoc boleh dilaksanakan sekiranya:	ICTSO IPKKM ICTSO Fasiliti

5.35 KAJIAN SEMULA KESELAMATAN MAKLUMAT SECARA BERKECUALI *(INDEPENDENT REVIEW OF INFORMATION SECURITY)*	**PERANAN**
(a) sebarang pindaan kepada undang-undang, garis panduan atau peraturan yang menjejaskan operasi keselamatan maklumat KKM; (b) peristiwa penting yang terjadi dan mempunyai kesan ke atas keselamatan maklumat, seperti kehilangan data dan pencerobohan; (c) usaha baharu atau perubahan yang besar dibuat di KKM; (d) KKM mengambil produk atau perkhidmatan baharu yang mempunyai implikasi keselamatan maklumat atau mengubah produk atau perkhidmatan sedia ada;dan (e) perubahan ketara dilaksanakan di pusat data KKM bagi kawalan keselamatan maklumat, peraturan dan proses.	
5.36 KEPATUHAN TERHADAP DASAR, PERATURAN, DAN STANDARD KESELAMATAN MAKLUMAT *(COMPLIANCE WITH POLICIES, RULES AND STANDARDS FOR INFORMATION SECURITY)*	**PERANAN**
5.36.1 Pematuhan Dasar, Peraturan dan Standard Keselamatan Maklumat Maklumat berkaitan dasar, peraturan dan piawaian keselamatan maklumat keseluruhan KKM perlu dikumpul supaya sentiasa tersedia sebagai rujukan apabila diperlukan. Perkara yang perlu dipertimbangkan apabila berlaku ketidak patuhan adalah seperti berikut: (a) mengenal pasti punca sebenar ketidakpatuhan; (b) menentukan tindakan pembetulan. (c) melaksanakan tindakan pembetulan untuk memastikan pematuhan berterusan; dan (d) menilai sebarang tindakan pembetulan yang diambil untuk melihat sama ada ia berkesan dan kenal pasti mana-mana elemen yang perlu diperbaiki.	ICTSO IPKKM ICTSO Fasiliti
5.37 DOKUMENTASI PROSEDUR *(DOCUMENTED OPERATING PROCEDURES)*	**PERANAN**
5.37.1 Dokumentasi Prosedur Operasi Prosedur Operasi pemprosesan maklumat perlu didokumenkan dan disediakan. Prosedur operasi berkaitan keselamatan maklumat perlu dibangunkan berdasarkan lima pertimbangan seperti berikut: (a) berlaku kes pertindihan kerja yang dilaksanakan oleh satu atau lebih individu; (b) apabila sesuatu kerja jarang/belum pernah dilaksanakan; (c) apabila terdapat prosedur yang berisiko dilupakan; (d) kerja baharu yang tidak biasa dilakukan oleh pegawai oleh itu mempunyai risiko yang lebih tinggi; dan (e) apabila tanggungjawab untuk menjalankan kerja dipindahkan kepada pekerja atau kumpulan pekerja yang berbeza. Apabila keadaan ini berlaku, prosedur operasi perlu menggariskan dengan jelas perkara berikut : (a) individu yang bertanggungjawab - sama ada penyandang atau pengendali baharu;	Pengurus ICT Penyelaras ICT Fasiliti

5.37 DOKUMENTASI PROSEDUR *(DOCUMENTED OPERATING PROCEDURES)*	PERANAN
(b) garis panduan untuk mengekalkan keselamatan semasa pemasangan dan konfigurasi mana-mana sistem perkhidmatan yang berkaitan; (c) bagaimana maklumat diproses sepanjang kerja dilakukan; (d) pelan dan implikasi BUDR sekiranya berlaku kehilangan data atau kejadian bencana (lihat Bab 8); (e) perlu ada hubungan antara kebergantungan dan mana-mana sistem lain, termasuk penjadualan; (f) prosedur yang jelas untuk menangani "ralat pengendalian" atau pelbagai peristiwa yang boleh berlaku (lihat Bab 8); (g) senarai lengkap pegawai untuk dihubungi sekiranya berlaku gangguan beserta prosedur menangani gangguan; (h) garis panduan operasi untuk media storan (rujuk Bab 7); (i) prosedur untuk reboot dan recover bagi kes kegagalan; (j) menyimpan log jejak audit termasuk log sistem dan peristiwa (events logs) (rujuk Bab 8). (k) sistem pemantauan untuk ruang kerja (rujuk Bab 7); dan (l) sistem pemantauan untuk memenuhi kapasiti operasi, potensi prestasi dan keselamatan kerja; dan Pendekatan di atas hendaklah tertakluk kepada semakan berkala dan/atau *ad-hoc* apabila diperlukan. Semua perubahan kepada prosedur hendaklah disahkan oleh pihak pengurusan dengan segera untuk melindungi semua aktiviti keselamatan maklumat yang dijalankan dalam KKM.	





6.0

BAB MANUSIA



6.1 TAPISAN KESELAMATAN *(SCREENING)*	PERANAN
6.1.1 Tapisan Keselamatan Tapisan keselamatan hendaklah dijalankan terhadap pegawai KKM, dan pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT di KKM yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang mesti dipatuhi ialah seperti yang berikut: (a) menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga KKM dan pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT KKM yang terlibat dalam menjamin keselamatan aset ICT; dan (b) mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.	Pengurus Sumber Manusia Pegawai KKM Pihak ketiga
6.2 SYARAT-SYARAT PEKERJAAN *(TERMS AND CONDITIONS OF EMPLOYMENT)*	**PERANAN**
6.2.1 Terma dan Syarat Perkhidmatan Persetujuan kontrak dengan KKM dan pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara yang mesti dipatuhi termasuk yang berikut: (a) menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai KKM serta pihak ketiga yang terlibat dalam menjamin keselamatan aset; dan (b) mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa berdasarkan perjanjian yang telah ditetapkan(tidak terhad kepada) seperti berikut: (i) perakuan untuk ditandatangani oleh penjawat awam berkenaan dengan Akta Rahsia Rasmi 1972; (ii) Surat Aku Janji; (iii) Borang *Non-Disclosure Agreement* (NDA); (iv) Borang Tapisan Keselamatan Kasar/Halus (Borang KPKK 11); (v) Surat Akuan Pematuhan PKS KKM; dan (vi) peraturan semasa yang sedang berkuatkuasa.	Pengurus Sumber Manusia
6.3 PROGRAM KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT *(INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING)*	**PERANAN**
6.3.1 Kesedaran, Pendidikan dan Latihan Pendidikan, kesedaran dan latihan keselamatan maklumat adalah komponen penting dalam strategi pengurusan risiko KKM. KKM perlu memastikan pegawai dilatih secukupnya untuk melaksanakan tugas tanpa menjejaskan keselamatan maklumat. Perkara yang boleh dipertimbangkan adalah seperti berikut: (a) membangunkan program kesedaran keselamatan maklumat, pendidikan dan latihan; (b) latihan boleh dijalankan melalui sama ada secara atas talian seperti video atau webinar atau secara fizikal;	Pengurus ICT Penyelaras ICT Fasiliti ICTSO IPKKM ICTSO Fasiliti Pegawai KKM

6.3 PROGRAM KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT *(INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING)*	PERANAN
memastikan program kesedaran, pendidikan dan latihan diberikan secara berterusan; (d) memperkenalkan program kesedaran, pendidikan dan latihan kepada pegawai baharu, pegawai bertukar peranan atau pegawai yang memerlukan; (e) kempen kesedaran perlu terdiri daripada pelbagai aktiviti untuk meningkatkan pemahaman. Ini boleh melibatkan kempen, booklet, poster, berita, laman web, sesi maklumat, taklimat, modul e-pembelajaran dan e-mel. Program yang dijalankan perlu mengambil kira perkara berikut: (a) melibatkan pihak pengurusan agar komitmen dapat diberikan untuk memastikan keselamatan maklumat di seluruh KKM; (b) pembudayaan kepada semua pihak dengan pematuhan kepada prosedur keselamatan maklumat yang berkaitan termasuk dasar keselamatan, peraturan, arahan, undang-undang, kontrak dan perjanjian tambahan mengenai keselamatan maklumat; (c) kepentingan akauntabiliti bagi tindakan yang diambil dan tindakan yang tidak diambil, tanggungjawab untuk melindungi maklumat milik KKM dan pihak berkepentingan; dan (d) mematuhi keselamatan asas seperti pelaporan insiden keselamatan maklumat dan kawalan garis dasar seperti keselamatan kata laluan.	
6.4 PROSES TATATERTIB *(DISCIPLINARY PROCESS)*	**PERANAN**
6.4.1 Proses Tatatertib Proses tatatertib yang formal perlu ditentukan dan disampaikan kepada pegawai atau pihak berkepentingan terlibat bagi membolehkan tindakan diambil ke atas pelanggaran dasar keselamatan maklumat yang dilakukan. KKM menetapkan dasar untuk melindungi data sulit, proprietari dan data peribadi seperti rekod pesakit dan rekod perubatan. Selain itu, dasar keselamatan komputer juga disertakan untuk memastikan data yang disimpan pada komputer kekal selamat dan tidak dapat dicapai tanpa kebenaran.	Pengurus ICT Pengurus Sumber Manusia ICTSO IPKKM ICTSO Fasiliti
6.4.2 Tujuan Tindakan Tatatertib Tujuan proses tatatertib adalah untuk memastikan pegawai dan mana-mana pihak lain yang berkepentingan memahami Langkah-langkah tatatertib hendaklah dilaksanakan dengan pantas apabila berlakunya pelanggaran dasar, untuk mengelakkan sebarang pelanggaran dasar KKM selanjutnya. Tindakan tatatertib mesti diambil apabila terdapat bukti ketidakpatuhan/ pelanggaran dasar, prosedur atau peraturan KKM. Ini juga termasuk mana-mana perundangan dan peraturan yang berkuatkuasa.	Pengurus ICT Pengurus Sumber Manusia ICTSO IPKKM
6.5 TANGGUNGJAWAB SELEPAS PENAMATAN ATAU PERTUKARAN PERKHIDMATAN *(RESPONSIBILITIES AFTER TERMINATION OR CHANGE OF EMPLOYMENT)*	**PERANAN**
6.5.1 Penjelasan Maklumat Tugas dan Tanggungjawab Peranan dan tanggungjawab berkaitan keselamatan maklumat yang masih	

6.5 TANGGUNGJAWAB SELEPAS PENAMATAN ATAU PERTUKARAN PERKHIDMATAN *(RESPONSIBILITIES AFTER TERMINATION OR CHANGE OF EMPLOYMENT)*	PERANAN
sah selepas penamatan atau pertukaran peranan/jawatan hendaklah ditentukan, dikuat kuasa dan disampaikan kepada warga KKM dan pihak ketiga Semua warga KKM dan pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT KKM yang telah tamat peranan/jawatan perlu mematuhi perkara-perkara berikut: (a) Memastikan semua aset maklumat milik KKM atau kerajaan dikembalikan kepada KKM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (c) Maklumat rasmi dalam aset maklumattidak dibenarkan dibawa keluar dari KKM. Warga KKM yang telah bertukar keluar KKM atau tamat perkhidmatan hendaklah: (a) Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada KKM mengikut (b) peraturan dan/atau terma perkhidmatan yang ditetapkan; (c) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (d) Menyediakan dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang menyatakan berkaitan aset/maklumat yang berkaitan.	Pengurus Sumber Manusia Pegawai KKM Pihak Ketiga
6.5.2 Pengurusan Pemberhentian atau Pertukaran Prosedur untuk menguruskan pemberhentian atau pertukaran pegawai perlu menyatakan tanggungjawab dan kewajipan pegawai berkaitan keselamatan maklumat yang masih berkuatkuasa selepas penamatan atau pertukaran tersebut. Ini mungkin termasuk mengekalkan kerahsiaan maklumat, harta intelek dan pengetahuan lain yang diperoleh, serta sebarang tanggungjawab lain yang ditetapkan oleh KKM. Tanggungjawab dan kewajipan yang kekal berkuatkuasa selepas penamatan pekerjaan, kontrak atau perjanjian individu hendaklah diperincikan dalam terma dan syarat. Selain itu, mana-mana kontrak atau perjanjian yang menjangkau tempoh tertentu selepas tamat pekerjaan individu tersebut turut perlu dinyatakan berkaitan tanggungjawab keselamatan maklumat. Antara perkara lain yang perlu disemak adalah seperti berikut: (a) memastikan semua aset yang dikembalikan kepada KKM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; (b) membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh KKM dan/atau terma perkhidmatan; dan (c) menguruskan urusan keluar, berhenti, pertukaran peranan dan tanggungjawab pengguna.	Pengurus Sumber Manusia Pegawai KKM Pihak Ketiga

6.6 PERJANJIAN KERAHSIAAN DAN KETIDAKDEDAHAN *(CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS)*	PERANAN
6.6.1 Perjanjian Kerahsiaan dan Ketidakdedahan Perjanjian kerahsiaan atau ketidakdedahan merupakan satu keperluan bagi KKM untuk melindungi maklumat. Perjanjian kerahsiaan atau ketidakdedahan perlu dikenal pasti, diperakui, dikaji secara berkala, dan ditandatangani oleh pegawai dan pihak berkepentingan yang berkaitan. Perjanjian/kontrak kerahsiaan dan non-disclosure agreement (NDA) mesti disediakan dengan tepat untuk melindungi semua rahsia dan data/maklumat sensitif yang berkaitan dengan aktiviti dan transaksi KKM. Adalah penting bahawa kedua-dua pihak memahami tugas dan tanggungjawab di bawah perjanjian semasa dan selepas berakhirnya perkhidmatan. Pegawai yang akan keluar atau yang bertukar hendaklah memindahkan tanggungjawab kepada pegawai yang baharu, dengan semua kelayakan capaian lama dibatalkan dan capaian baharu diwujudkan.	Pengurus Sumber Manusia Pengurus ICT Penyelaras ICT Fasiliti ICTSO IPKKM ICTSO Fasiliti
6.7 BEKERJA SECARA JARAK JAUH *(REMOTE WORKING)*	**PERANAN**
6.7.1 Bekerja Secara Jarak Jauh Langkah-langkah keselamatan perlu dilaksanakan apabila pegawai bekerja dari jauh bagi melindungi maklumat yang dicapai, diproses atau disimpan di luar premis KKM. KKM mesti memastikan mereka mempunyai perlindungan yang diperlukan untuk mendapatkan maklumat sensitif atau sulit yang dihantar atau disimpan secara elektronik semasa operasi dari jauh. Perkara berikut perlu diambil kira: (a) komunikasi yang selamat mesti dipastikan dengan mengambil kira terhadap keperluan capaian jarak jauh dari luar KKM, sensitiviti data yang dipindahkan, dan kelemahan sistem aplikasi; (b) menyediakan peraturan atau larangan yang berkaitan penggunaan perkhidmatan rangkaian tanpa wayar bagi tujuan bekerja dari luar pejabat, samada di rumah atau tempat awam; (c) peraturan atau larangan yang berkaitan penggunaan perkhidmatan rangkaian tanpa wayar bagi pekerjaan di kedua-dua lokasi rangkaian di rumah dan tempat awam; (d) menyediakan langkah keselamatan, seperti *firewall* dan perlindungan anti-malware; (e) memastikan sistem boleh digunakan dan dimulakan dari jauh menggunakan protokol yang selamat; dan (f) mekanisme pengesahan selamat mesti diaktifkan untuk memberikan capaian istimewa, dengan mengambil kira kerentanan mekanisme pengesahan satu-faktor apabila capaian dari jauh ke rangkaian KKM dibenarkan.	Pengurus Sumber Manusia Pengurus ICT ICTSO IPKKM ICTSO Fasiliti
6.8 PELAPORAN PERISTIWA KESELAMATAN MAKLUMAT *(INFORMATION SECURITY EVENT REPORTING)*	**PERANAN**
6.8.1 Pelaporan Peristiwa Keselamatan Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat berdasarkan pekeliling atau prosedur pengendalian insiden yang sedang berkuatkuasa. Perkara yang perlu	

6.8 PELAPORAN PERISTIWA KESELAMATAN MAKLUMAT *(INFORMATION SECURITY EVENT REPORTING)*	PERANAN
dipatuhi ialah seperti yang berikut: (a) menentukan mekanisme untuk melaporkan sebarang insiden melalui saluran dan dalam tempoh masa yang ditentukan; (b) memberi kesedaran berkaitan prosedur pengendalian insiden dan hebahan kepada pegawai KKM sekiranya terdapat perubahan; (c) memastikan pegawai KKM yang mengurus insiden mempunyai kompetensi yang diperlukan; dan (d) Insiden keselamatan ICT atau ancaman yang berlaku hendaklah dilaporkan kepada CSIRT KKM berdasarkan prosedur pengendalian insiden yang sedang berkuatkuasa. Kawalan ini memerlukan perkara berikut: (a) setiap pegawai perlu memahami kewajipan untuk melaporkan insiden keselamatan maklumat dengan segera untuk menghentikan atau mengurangkan kesannya; (b) KKM mesti mengekalkan rekod personal untuk dihubungi bagi melaporkan insiden keselamatan data dan memastikan proses itu mudah, boleh dicapai dan tersedia; (c) KKM mesti menyimpan rekod insiden keselamatan maklumat seperti laporan insiden, log peristiwa, permintaan perubahan, laporan masalah dan dokumentasi sistem. Selain itu, bukan tanggungjawab pegawai yang melaporkan untuk menguji ketahanan terhadap sebarang insiden keselamatan. Ianya perlu diserahkan kepada pegawai yang berkelayakan untuk mengendalikannya kerana boleh mengakibatkan liabiliti undang-undang.	Pegawai KKM CSIRT IPKKM CSIRT Fasiliti KKM ICTSO IPKKM ICTSO Fasiliti




"...tahniah anda selesai
membaca sehingga disini..."
"...sambung bab
seterusnya disebelah..."



7.0



BAB FIZIKAL



7.1 PERIMETER KESELAMATAN FIZIKAL (PHYSICAL SECURITY PERIMETERS)	PERANAN
7.1 Perimeter Keselamatan Fizikal Keselamatan fizikal merujuk kepada langkah-langkah perlindungan fizikal bagi menjaga premis KKM serta melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat yang sensitif atau kritikal. Ia bertujuan untuk menghalang capaian tanpa kebenaran, kerosakan dan gangguan secara fizikal terhadap premis dan aset KKM. Perkara yang perlu dipatuhi adalah seperti berikut: (a) kawasan yang memerlukan kawalan keselamatan fizikal hendaklah dikenal pasti. Lokasi dan kawalan hendaklah bergantung pada keperluan untuk melindungi aset hasil dari penilaian risiko; (b) menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (c) memasang alat penggera atau kamera keselamatan; (d) menghadkan jalan keluar masuk; (e) mengadakan kaunter kawalan jika perlu; (f) menyediakan tempat atau bilik khas untuk pelawat-pelawat; (g) mewujudkan perkhidmatan kawalan keselamatan; (h) melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan pegawai yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (i) mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; (j) mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau bilau manusia dan sebarang bencana; (k) melaksana perlindungan fizikal dan menyediakan garis panduan untuk pegawai yang bekerja di dalam kawasan terhad; (l) memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan (m) merekod pelawat secara elektronik" jika perlu dan melaksanakan kawalan log audit fizikal secara berkala untuk capaian ke kawasan kritikal. Perkara ini diperlukan bagi menghalang: (a) kemasukan tanpa kebenaran ke dalam bangunan, bilik atau kawasan yang mengandungi aset maklumat; (b) penyingkiran aset tanpa kebenaran dari premis; (c) penggunaan aset premis tanpa kebenaran seperti komputer dan peranti berkaitan; dan (d) mengganggu peralatan komunikasi elektronik yang tidak dibenarkan, seperti telefon, dan terminal komputer.	CDO Pengurus ICT Penyelaras ICT Fasiliti
7.2 KEMASUKAN FIZIKAL *(PHYSICAL ENTRY)*	**PERANAN**
7.2.1 Kemasukan Fizikal KKM mesti mengawal dan, jika boleh, mengasingkan	

7.2 KEMASUKAN FIZIKAL *(PHYSICAL ENTRY)*	PERANAN
kawasan seperti kawasan penghantaran,pemunggahan dan pintu masuk lain ke premis daripada fasiliti ICT untuk menghalang kemasukan tanpa kebenaran. Oleh itu, laluan masuk yang diperlukan sahaja perlu disediakan untuk menjamin hanya pegawai yang diberi kuasa boleh memasuki kawasan terkawal. Kawalan hendaklah dilaksanakan untuk menjamin bahawa hanya orang yang diberi kuasa mempunyai kebenaran, dan mereka perlu dikenal pasti dan disahkan. Penggunaan kawalan, kunci (manual dan elektronik), pengawal keselamatan, sistem pemantauan, dan halangan lain di pintu masuk perlu dilaksanakan. Sistem kawalan capaian seperti kata laluan,akses kad atau peranti biometrik perlu digunakan untuk melindungi kawasan sensitif dalam fasiliti. Perkara yang perlu dipatuhi adalah seperti berikut: (a) setiap pegawai KKM hendaklah memakai atau mempamerkan pas keselamatan sepanjang waktu bertugas; (b) semua pas keselamatan hendaklah diserahkan semula kepada KKM apabila pegawai tersebut bertukar keluar, tamat perkhidmatan atau bersara; (c) setiap pelawat hendaklah merekodkan maklumat dan tujuan lawatan di dalam Buku Rekod Pelawat atau apa-apa kaedah rekod yang digunakan di KKM dan mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama premis KKM. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan (d) kehilangan pas mestilah dilaporkan dengan segera.	Pengurus ICT Penyelaras ICT Fasiliti ICTSO

7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN *(SECURING OFFICES, ROOMS AND FACILITIES)*	PERANAN
7.3.1 Keselamatan Pejabat, Bilik dan Kemudahan Kawalan bagi melindungi maklumat KKM dan aset lain yang berkaitan daripada capaian fizikal yang tidak dibenarkan, kerosakan dan gangguan di pejabat, bilik, dan kemudahan hendaklah dirangka dan dilaksanakan. Kawalan ini perlu bagi mengurangkan risiko capaian fizikal yang tidak dibenarkan di pejabat, bilik dan kemudahan ke tahap yang boleh diterima dengan: (a) menghalang individu yang tidak dibenarkan daripada memasuki pejabat, bilik atau kemudahan. Semua pegawai mesti diberi kuasa sebelum mendapatkan capaian; (b) mencegah bahaya atau gangguan kepada data KKM dan aset lain yang berkaitan dalam kawasan, bilik dan kemudahan tempat kerja; (c) meminimumkan kemungkinan kecurian atau kehilangan harta benda di pejabat, bilik dan kemudahan; (d) memastikan pengenalan pegawai yang dibenarkan sahaja untuk mencapai secara fizikal melalui pemakaian pakaian seragam, sistem kemasukan pintu elektronik dan pas pelawat; dan (e) CCTV atau sistem pengawasan lain perlu dilaksanakan untuk memastikan keselamatan di kawasan penting seperti pintu/keluar di kawasan yang bersesuaian.	Pengurus ICT Penyelaras ICT Fasiliti ICTSO

7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN *(SECURING OFFICES, ROOMS AND FACILITIES)*	PERANAN
Keperluan bagi memenuhi kawalan ini adalah seperti berikut: (a) mengenal pasti kemudahan kritikal untuk menghalang capaian orang ramai; (b) memastikan bangunan memberikan petunjuk yang minimum tentang tujuannya, tanpa penanda yang jelas sama ada di dalam atau di luar bangunan yang menunjukkan aktiviti pemprosesan maklumat sedang berlaku; (c) menyediakan sistem untuk melindungi data dan aktiviti sulit daripada didengar atau dilihat dari luar; dan (d) memastikan direktori, buku telefon dalaman dan peta dalam talian yang menunjukkan lokasi kemudahan pemprosesan maklumat sulit tidak boleh dicapai oleh mana-mana individu yang tidak dibenarkan.	
7.4 PEMANTAUAN KESELAMATAN FIZIKAL *(PHYSICAL SECURITY MONITORING)*	**PERANAN**
7.4.1 Pemantauan Keselamatan Fizikal KKM perlu melaksanakan penggunaan alat pengawasan yang sesuai. Ini adalah untuk mengesan dan menghalang penceroboh luar dan dalam daripada memasuki kawasan fizikal larangan tanpa kebenaran. Jenis-jenis pemantauan keselamatan yang ada adalah seperti: (a) kamera CCTV; (b) pengawal keselamatan; (c) sistem amaran pencerobohan; dan (d) perisian pengurusan keselamatan fizikal. Bagi mengesan dan menghalang capaian tanpa kebenaran kepada kemudahan yang menempatkan aset maklumat kritikal dan mengelakkannya daripada dikompromi, KKM boleh mempertimbangkan untuk : (a) meletakkan Sistem Pemantauan Video untuk terus memantau capaian ke kawasan larangan yang menjadi simpanan aset maklumat kritikal; (b) memasang sistem pengawasan video, seperti kamera CCTV. Sistem pengawasan ini penting untuk menyimpan rekod semua kemasukan dan keluar di premis; dan (c) memasang pengesan untuk mencetuskan Penggera Amaran. Keupayaan untuk mencetuskan penggera apabila penceroboh memasuki premis fizikal membolehkan pasukan keselamatan bertindak balas dengan cepat terhadap sebarang pelanggaran keselamatan. Untuk menghalang penceroboh daripada memasuki premis, adalah disyorkan agar KKM memasang alat pengesan gerakan, bunyi dan sentuhan yang akan memberi amaran apabila aktiviti tidak normal dikesan dalam premis fizikal KKM. Ini termasuk, tetapi tidak terhad kepada: (a) pengesan sentuhan perlu dipasang di persekitaran premis. Apabila objek atau individu yang tidak diketahui bersentuhan dengan objek tertentu atau memutuskan sentuhan dengan objek tertentu, penggera perlu diaktifkan. Pengesan sentuhan boleh, sebagai contoh, dikonfigurasikan untuk mencetuskan penggera apabila pengesan ini bersentuh dengan mana-mana tingkap atau pintu;	Pengurus ICT Penyelaras ICT Fasiliti

7.4 PEMANTAUAN KESELAMATAN FIZIKAL *(PHYSICAL SECURITY MONITORING)*	PERANAN
(b) pengesan gerakan boleh dikonfigurasikan untuk memberi amaran kepada petugas jika mereka mengesan pergerakan dalam kawasan pandangan yang dikhaskan terhadap objek yang bergerak dalam kawasan tersebut; dan (c) pengesan bunyi, seperti pengesan kaca pecah, boleh diaktifkan apabila ia mengesan bunyi, yang boleh membantu mencegah perkara tidak normal.	
7.4.2 Konfigurasi Penggera untuk Semua Premis Dalaman Adalah penting untuk memastikan bahawa sistem penggera telah dikonfigurasikan dengan sewajarnya. Ini akan memastikan semua kawasan sensitif, termasuk semua pintu luar, tingkap, kawasan tidak berpenghuni dan bilik komputer berada dalam lingkungan sistem penggera. Ini akan menghalang sebarang kelemahan daripada disalah guna.	ICTSO
7.5 PERLINDUNGAN DARIPADA ANCAMAN FIZIKAL DAN ALAM SEKITAR *(PROTECTING AGAINST PHYSICAL AND ENVIRONMENTAL THREATS)*	**PERANAN**
7.5.1 Perlindungan dari Ancaman Fizikal dan Persekitaran KKM perlu merangka dan melaksanakan perlindungan fizikal terhadap bencana alam seperti kebakaran, banjir, letupan, kacau bilau, serangan berniat jahat atau kemalangan seperti penyediaan latihan kecemasan berkala (drill), Pelan Kesinambungan Perkhidmatan (PKP) dan Pelan Pemulihan Bencana.	Pengurus ICT Penyelaras ICT Fasiliti
7.6 BEKERJA DI KAWASAN TERKAWAL *(WORKING IN SECURE AREAS)*	**PERANAN**
7.6 Bekerja di Kawasan Terkawal Prosedur bekerja di kawasan terkawal hendaklah dirangka dan dilaksanakan. Kawasan terkawal ditakrifkan sebagai kawasan yang dihadkan kepada pegawai tertentu sahaja yang melibatkan Maklumat Rahsia Rasmi. Ini dilaksanakan untuk melindungi aset yang terdapat di dalam kawasan tersebut. Perkara yang perlu dipatuhi adalah seperti berikut: (a) capaian kepada kawasan terkawal hanya kepada pegawai yang dibenarkan sahaja; (b) pihak ketiga adalah dilarang untuk memasuki kawasan terkawal kecuali dengan kebenaran untuk kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal dan hendaklah di pantau sehingga tugas di kawasan berkenaan selesai; (c) kawasan terkawal perlu dikunci pada setiap masa; (d) pemantauan dibuat menggunakan CCTV kamera atau lain-lain peralatan yang sesuai; (e) peralatan keselamatan (CCTV, log capaian) perlu diperiksa secara berjadual; (f) fotografi, video, audio dan peralatan rakaman lain tidak dibenarkan dibawa masuk; dan (g) pegawai dan pihak ketiga yang perlu berurusan di pusat data hendaklah mendapatkan kebenaran dan mengisi buku log keluar masuk kawasan terkawal.	Pengurus ICT Penyelaras ICT Fasiliti

7.7 POLISI MEJA SELAMAT DAN PAPARAN SELAMAT *(CLEAR DESK AND CLEAR SCREEN)*	PERANAN
7.7.1 Polisi Meja dan Paparan Selamat Polisi *Clear Desk* untuk dokumen dan media penyimpanan boleh alih serta Polisi *Clear Screen* untuk kemudahan pemprosesan maklumat hendaklah dipatuhi. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara yang perlu dipertimbangkan oleh KKM apabila mewujudkan dan menguatkuasakan dasar *Clear Desk* Dan *Clear Screen* adalah seperti berikut: (a) peralatan ICT yang mengandungi maklumat sensitif atau kritikal perlu dikunci dengan selamat apabila tidak digunakan atau apabila stesen kerja ditinggalkan; (b) peralatan ICT yang digunakan seperti komputer riba, pengimbas, pencetak dan buku nota, perlu dilindungi dengan kunci kekunci apabila tidak digunakan atau dibiarkan tanpa pengawasan; (c) pegawai perlu memastikan peralatan ICT mereka dilog keluar apabila meninggalkan ruang kerja dan meninggalkannya tanpa pengawasan. Mengaktifkan semula peranti hanya boleh dilakukan dengan pengesahan pengguna. Semua peranti seperti komputer, perlu mempunyai ciri tamat masa dan log keluar automatik; (d) pencetak hendaklah dikonfigurasi supaya cetakan boleh diambil dan diterima dengan segera oleh orang yang mencetaknya (pemilik). (e) bahan yang mengandungi maklumat sensitif termasuk media storan boleh dibuang hendaklah disimpan dengan selamat pada setiap masa. Apabila tidak lagi memerlukannya, ia hendaklah dilupuskan dengan cara yang selamat; (f) memaparkan pop-up atau apa-apa kaedah pemakluman pada skrin bagi menyampaikan peraturan ini kepada semua pegawai yang berkaitan; (g) papan putih perlu dipadamkan apabila maklumat sensitif atau kritikal tidak lagi diperlukan; (h) menambahkan pengaktifan kunci skrin pada peranti bagi tujuan keselamatan selepas 5 minit atau berdasarkan tetapan organisasi; dan (i) melaksanakan kempen kesedaran bulanan berkaitan perkara diatas.	Pengguna Pegawai KKM ICTSO IPKKM ICTSO Fasiliti
7.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN *(EQUIPMENT SITING AND PROTECTION)*	**PERANAN**
7.8.1 Penempatan dan Perlindungan Peralatan ICT Peralatan ICT hendaklah ditentukan penempatannya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran, serta ancaman penyalahgunaan capaian. KKM perlu mengasingkan peralatan ICT daripada peralatan yang tidak dimiliki atau dikawal oleh KKM.	

7.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN *(EQUIPMENT SITING AND PROTECTION)*	PERANAN
Perkara yang perlu dipatuhi adalah seperti berikut: (a) pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; (b) pengguna bertanggungjawab sepenuhnya ke atas peralatan ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang ditetapkan; (c) pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang peralatan ICT yang telah ditetapkan; (d) pengguna dilarang membuat pemasangan sebarang perisian tambahan tanpa kebenaran Ketua Jabatan/Pegawai ICT; (e) pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; (f) pengguna mesti memastikan perisian antivirus di dalam peralatan ICT sentiasa aktif dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; (g) penggunaan kata laluan untuk capaian ke sistem komputer adalah diwajibkan; (h) semua aset sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; (i) peralatan-peralatan kritikal perlu disokong oleh UPS dan Generator Set (Gen-Set); (j) semua peralatan ICT 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 dalam rak khas dan berkunci; (k) semua peralatan ICT yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai; (l) menambah keperluan pemantauan suhu dan kelembapan bilik server serta menyediakan sokongan amaran automatik melalui sistem pemantauan. (m) peralatan ICT yang hendak dibawa keluar dari premis, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan; (n) peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera; (o) pengendalian aset hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa; (p) pengguna tidak dibenarkan mengubah kedudukan peralatan ICT dari tempat asal ia ditempatkan tanpa kebenaran Ketua Jabatan/Pegawai ICT /Penyelaras ICT; (q) sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk baik pulih; (r) sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin aset tersebut sentiasa berkeadaan baik; (s) konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;	Pegawai KKM Pentadbir Aset Pegawai Aset Pegawai Kejuruteraan

7.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN *(EQUIPMENT SITING AND PROTECTION)*	PERANAN
(t) pengguna dilarang sama sekali mengubah kata laluan pentadbir (administrator password) yang telah ditetapkan oleh Pentadbir Sistem ICT; (u) pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (v) pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan OFF apabila meninggalkan pejabat; dan (w) memastikan plug dicabut daripada suis utama (main switch) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
7.9 KESELAMATAN ASET DI LUAR PREMIS *(SECURITY OF ASSETS OFF-PREMISES)*	**PERANAN**
7.9.1 Keselamatan Aset di Luar Premis Peralatan yang mengandungi aset maklumat berharga dialih keluar dari lokasi fizikal KKM lebih mudah terdedah kepada bahaya, kecurian, kehilangan, kemusnahan atau pelanggaran polisi. Kawalan keselamatan fizikal dalam premis KKM tidak dapat dilaksanakan menyebabkan aset diluar premis terdedah kepada ancaman pelbagai risiko. KKM perlu melindungi keselamatan aset maklumat yang disimpan dalam peralatan yang dibawa keluar dari premis KKM dengan memberi perhatian terhadap risiko seperti berikut: (a) peralatan perlu dilindungi dan dikawal sepanjang masa; (b) penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan (c) keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan; dan (d) KKM perlu memasang alat penjejakan lokasi dan remote access, supaya lokasi peranti boleh dipantau dan, jika perlu, sebarang data yang disimpan pada peranti boleh dipadam dari jauh. (e) aset mudah alih perlu didaftarkan dalam sistem aset dan ditetapkan tempoh pemantauan penggunaan luar (contoh: audit bulanan). (f) peralatan ICT yang hendak dibawa keluar dari premis KKM untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Jabatan atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan	Pentadbir Aset Pegawai Aset
7.10 PENYIMPANAN MEDIA *(STORAGE MEDIA)*	**PERANAN**
7.10.1 Pengurusan Media Untuk mengelakkan kerosakan pada aset maklumat media boleh alih harus dikawal dan dilindungi secara fizikal. Media boleh alih mesti dikendalikan mengikut pengelasan maklumat. **Media Storan Boleh Alih** Media boleh alih amat diperlukan untuk pelbagai operasi perkhidmatan dan digunakan secara meluas oleh pegawai. Walau bagaimanapun, ia	

7.10 PENYIMPANAN MEDIA *(STORAGE MEDIA)*	PERANAN
menimbulkan risiko tertinggi kepada data sensitif. Polisi dan prosedur penyulitan (encryption) media storan sensitif perlu dimasukkan sebagai mandatori. Kawalan yang perlu dipatuhi oleh KKM untuk pengurusan media storan boleh alih semasa kitaran hayatnya adalah seperti berikut: (a) KKM perlu mewujudkan dasar yang tertumpu pada pemerolehan, kebenaran, penggunaan dan pelupusan media storan boleh alih, seterusnya memaklumkan semua pegawai dan pihak berkenaan tentang kewujudannya; (b) KKM hendaklah, apabila perlu melaksanakan prosedur kebenaran untuk mengambil media storan boleh alih keluar dari premis . Selain itu, log penyingkiran hendaklah disimpan untuk penjejakan audit; (c) simpan semua media storan di tempat yang selamat seperti peti besi, dengan mengambil kira tahap pengelasan maklumat yang diberikan kepada maklumat dan sebarang ancaman alam sekitar dan fizikal kepada media; (d) kaedah kriptografi perlu digunakan untuk melindungi media daripada capaian tanpa kebenaran bagi mengekalkan kerahsiaan dan kebolehpercayaan maklumat yang terdapat dalam media boleh alih; (e) untuk mengelakkan kemerosotan jangka hayat media storan boleh alih dan kehilangan data, maklumat itu hendaklah dialihkan ke peranti media storan baharu sebelum risiko wujud; (f) penting untuk menyalin dan menyimpan data sensitif pada beberapa media storan untuk mengurangkan peluang maklumat kritikal hilang; (g) pemantauan pemindahan maklumat ke mana-mana peranti media storan boleh tanggal perlu dibuat; dan (h) mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan.	Pentadbir Aset Pegawai Aset
7.10.2 Panduan Bagi Penggunaan Semula Secara Terkawal Dan Pelupusan Media Storan KKM perlu membuat perancangan sekiranya ingin mengitar semula dan melupuskan media storan dengan mengambil kira pengelasan data yang disimpan dalam media storan. KKM perlu mempertimbangkan perkara berikut: (a) pihak KKM yang ingin menggunakan semula media storan, maklumat sensitif yang disimpan padanya hendaklah dipadamkan atau diformat semula secara tidak boleh ditarik balik sebelum dibenarkan untuk digunakan; (b) media yang mengandungi maklumat terperingkat hendaklah disanitasi terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa. (c) pemusnahan terkawal media storan yang menyimpan maklumat sensitif adalah perlu apabila ia tidak lagi diperlukan. Dokumen kertas boleh dicincang dan peralatan digital boleh dimusnahkan secara fizikal; (c) pemusnahan terkawal media storan yang menyimpan maklumat sensitif adalah perlu apabila ia tidak lagi diperlukan. Dokumen kertas	Pentadbir Aset Pegawai Aset

7.10 PENYIMPANAN MEDIA *(STORAGE MEDIA)*	PERANAN
boleh dicincang dan peralatan digital boleh dimusnahkan secara fizikal; (c) pemusnahan terkawal media storan yang menyimpan maklumat sensitif adalah perlu apabila ia tidak lagi diperlukan. Dokumen kertas boleh dicincang dan peralatan digital boleh dimusnahkan secara fizikal; (d) KKM perlu menjalankan pemilihan pihak ketiga untuk mengumpul dan melupuskan media storan dengan memastikan pihak yang dipilih adalah cekap dan mempunyai kawalan yang sewajarnya; (e) mendokumentasikan semua media storan yang dilupuskan untuk jejak audit; dan (f) apabila melupuskan beberapa media storan bersama-sama, pertimbangan perlu diberikan kepada kesan kumulatif: Penggabungan pelbagai cebisan data daripada setiap medium storan boleh mengakibatkan perubahan maklumat dari tidak sensitif kepada bahan sensitif. KKM perlu menilai risiko data sulit yang disimpan pada peralatan yang rosak, untuk menentukan sama ada peralatan itu perlu dimusnahkan atau dibaiki.	
7.11 UTILITI SOKONGAN *(SUPPORTING UTILITIES)*	**PERANAN**
7.11.1 Utiliti Sokongan Fasiliti pemprosesan maklumat perlu dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. KKM hendaklah menambah keperluan pemantauan beban kuasa (power surge monitoring) dan penggunaan auto-transfer switch bagi fasiliti kritikal, serta memastikan peranan kejuruteraan dilibatkan dalam pelaksanaan, pemantauan dan penyelenggaraan kawalan ini. KKM perlu mempertimbangkan perkara berikut: (a) semua alat sokongan bagi aset maklumat perlu diselenggara dari semasa ke semasa (b) audit utiliti adalah perlu untuk memastikan bahawa ia mematuhi objektif dan serasi dengan utiliti lain; (c) utiliti peralatan sokongan perlu menjalani pemeriksaan dan ujian berkala untuk mengelakkan gangguan atau kegagalan; (d) sistem penggera ke atas peralatan utiliti yang tidak berfungsi boleh dilaksanakan berdasarkan tahap risiko aset maklumat dan kesinambungan perkhidmatan;	Pentadbir Aset Pegawai Aset Pegawai Kejuruteraan
7.12 KESELAMATAN KABEL *(CABLING SECURITY)*	**PERANAN**
7.12.1 Keselamatan Kabel Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Kabel termasuk kabel elektrik atau telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi.	

7.12 KESELAMATAN KABEL *(CABLING SECURITY)*	PERANAN
Sebagai langkah tambahan, KKM hendaklah melaksanakan langkah berikut: (a) pemantauan fizikal ke atas laluan dan keadaan kabel; (b) pemetaan lokasi kabel secara digital untuk tujuan rujukan dan kawalan keselamatan; (c) menjalankan audit keselamatan kabel secara tahunan bagi memastikan keberkesanan kawalan. KKM dinasihatkan untuk mempertimbangkan kriteria pematuhan berikut: (a) kabel telekomunikasi dan kabel kuasa yang menyambung ke kemudahan pemprosesan maklumat perlu ditanam di bawah tanah. Kabel yang ditanam di bawah tanah perlu dilindungi daripada pemotongan tidak sengaja menggunakan teknik yang sesuai seperti armored conduits. Langkah perlindungan alternatif, seperti tiang utiliti dan pelindung kabel lantai, boleh dipertimbangkan jika penempatan di bawah tanah tidak dapat dilaksanakan; (b) kabel kuasa dan komunikasi perlu diasingkan untuk menghapuskan risiko gangguan; (c) untuk melindungi aset maklumat sensitif dan operasi perkhidmatan, KKM perlu mempertimbangkan kawalan berikut untuk kabel yang disambungkan ke sistem maklumat kritikal: (i) memasang armored conduits, memasang bilik dan kotak berkunci, dan menyediakan sistem penggera di terminal dan tempat pemeriksaan; (ii) penggunaan teknik perisai ber-elektromagnet untuk mengelakkan kabel daripada rosak; (iii) pemeriksaan kabel dan semakan teknikal yang kerap perlu dijalankan untuk memastikan tiada peranti yang tidak dibenarkan disambungkan ke kabel; (iv) menetapkan prosedur dan langkah bagi mengawal capaian ke bilik kabel dan patch panel; dan (v) menggunakan kabel gentian optik. (d) maklumat dan destinasi kabel hendaklah dilabelkan untuk memudahkan pengenalpastian dan pemeriksaan pada kedua-dua permulaan dan akhir setiap kabel. Selain itu, KKM digalakkan untuk mendapatkan nasihat profesional pengurusan risiko berkaitan dengan kerosakan kabel. Perkara lain yang perlu dipertimbangkan ialah risiko yang berkaitan dengan penggunaan kabel komunikasi dan kuasa di premis yang sama oleh pelbagai organisasi.	Pengurus ICT Penyelaras ICT Fasiliti Pentadbir Rangkaian

7.13 PENYELENGGARAAN PERALATAN *(EQUIPMENT MAINTENANCE)*	PERANAN
7.13.1 Penyelenggaraan Peralatan Peralatan perlu dijaga dengan betul untuk memastikan ketersediaan, integriti, dan kerahsiaan maklumat. Langkah dan prosedur perlu dilaksanakan untuk memastikan aset maklumat dilindungi daripada kehilangan, kerosakan dan capaian tanpa kebenaran. Langkah-langkah kawalan keselamatan yang boleh dilaksanakan adalah seperti berikut::	

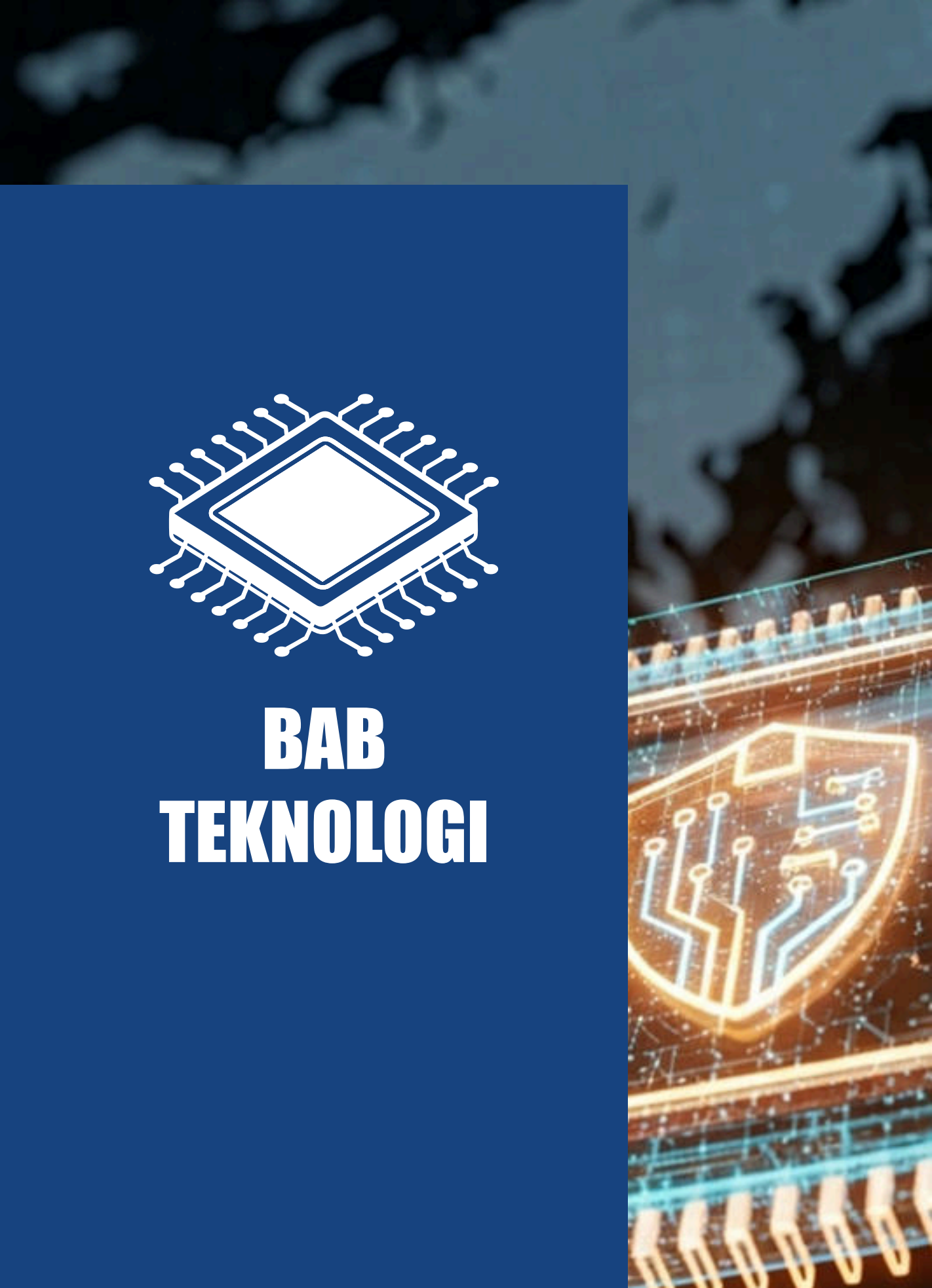
7.12 KESELAMATAN KABEL *(CABLING SECURITY)*	PERANAN
(a) digalakkan mematuhi spesifikasi pengeluar peralatan berkenaan prosedur penyelenggaraan seperti selang penyelenggaraan yang disyorkan; (b) penggunaan Borang Kebenaran Kerja Penyelenggaraan (Work Permit Form) adalah diwajibkan bagi semua pihak ketiga yang menjalankan kerja penyelenggaraan; (c) untuk semua peralatan, KKM perlu mewujudkan dan melaksanakan program penyelenggaraan; (d) menyelenggara atau membaiki peralatan hanya boleh dilakukan oleh pegawai yang diberi kuasa atau pihak ketiga yang disahkan; (e) semua kerosakan dan peralatan yang tidak berfungsi hendaklah direkodkan oleh KKM. Perlu diingatkan semua aktiviti penyelenggaraan pada peralatan tersebut juga perlu direkodkan; (f) penting bagi jabatan untuk menggunakan prosedur penyelenggaraan yang sesuai tanpa mengira sama ada penyelenggaraan dilakukan oleh pegawai atau pihak ketiga. Perjanjian kerahsiaan hendaklah ditandatangani oleh pegawai yang terlibat; (g) semua pegawai penyelenggaraan hendaklah diawasi pada setiap masa; (h) prosedur capaian dan kebenaran perlu dikuatkuasakan dengan ketat untuk kerja penyelenggaraan secara jarak jauh; (i) jabatan hendaklah menggunakan langkah keselamatan yang sesuai apabila peralatan dialihkan dari premis untuk penyelenggaraan; (j) keperluan penyelenggaraan yang ditetapkan penyedia insurans perlu dipatuhi oleh KKM; (k) untuk memastikan peralatan tidak terganggu dan berfungsi dengan baik, KKM perlu memeriksanya selepas penyelenggaraan;dan (l) KKM hendaklah mewujudkan dan melaksanakan langkah dan prosedur yang sesuai untuk melupuskan atau menggunakan semula peralatan.	Pengurus ICT Penyelaras ICT Fasiliti Pemilik Aset Pemilik Sistem
7.14 PELUPUSAN ATAU PENGGUNAAN SEMULA PERALATAN DENGAN SELAMAT *(SECURE DISPOSAL OR RE-USE OF EQUIPMENT)*	**PERANAN**
7.14.1 Pelupusan atau Penggunaan Semula Peralatan Peralatan yang mengandungi media storan perlu diperiksa untuk memastikan bahawa sebarang data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (overwrite) sebelum dilupuskan atau diguna semula. Peralatan aset maklumat yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuatkuasa. Pelupusan perlu dilakukan secara terkawal dan sempurna supaya maklumat tidak terlepas daripada kawalan KKM. Kawalan ini menetapkan beberapa perkara yang perlu pertimbangan untuk pematuhan seperti berikut: (a) sebelum pelupusan atau penggunaan semula, jabatan perlu memastikan peralatan yang mempunyai sebarang aset maklumat dan perisian	

7.12 KESELAMATAN KABEL *(CABLING SECURITY)*	PERANAN
berlesen dihapuskan secara kekal; (b) dua (2) pendekatan boleh diambil untuk memastikan pelupusan peralatan dengan cara yang selamat dan kekal adalah seperti berikut: (i) peralatan ICT yang mempunyai peranti media storan dan mengandungi maklumat hendaklah disanitasi dengan secara logikal, fizikal dan kaedah-kaedah lain sanitasi yang boleh dipertimbangkan dan sesuai digunakan semula atau dilupuskan secara fizikal;; dan (ii) jabatan hendaklah merujuk kepada kawalan ini dan Bab 8 berkenaan Media Penyimpanan dan Sanitasi, untuk memastikan semua data yang disimpan pada peralatan dipadamkan, ditulis ganti atau dihapuskan bagi menghalang pengambilan semula oleh pihak yang berniat jahat. (c) bagi komponen peralatan dan data yang terkandung di dalamnya yang dilabel atau ditanda bagi memudahkan untuk dikenal pasti pemilik aset, atau tahap pengelasan maklumat, semua label dan tanda ini hendaklah dimusnahkan secara kekal; dan (d) Jabatan boleh mempertimbangkan untuk menyahpasang kawalan keselamatan, seperti sekatan capaian atau sistem pengawasan, apabila mengosongkan kemudahan di fasiliti, dengan syarat berikut: (i) perjanjian yang menetapkan syarat untuk pemulangan harta tersebut; (ii) perlu mengurangkan risiko sebarang capaian tanpa kebenaran kepada maklumat sensitif oleh penyewa/penduduk pada masa akan datang; dan (iii) kawalan semasa dapat digunakan di kemudahan yang akan datang.	ICTSO IPKKM ICTSO Fasiliti Pengurus ICT Penyelaras ICT Fasiliti Pegawai Aset





8.0



BAB
TEKNOLOGI

8.1 PERANTI TITIK AKHIR PENGGUNA *(USER ENDPOINT DEVICES)*	PERANAN
8.1.1 Penggunaan Peranti Titik Akhir Pengguna *(Endpoint Devices)* Peranti Titik Akhir Pengguna seperti komputer riba, telefon mudah alih dan tablet terdedah kepada ancaman siber. Penjenayah siber sering memanfaatkan peranti ini untuk mendapatkan capaian tidak sah kepada perkhidmatan rangkaian dan boleh mengakibatkan kebocoran maklumat sulit. KKM perlu mewujudkan polisi bagi meliputi konfigurasi terkawal dan penggunaan peranti titik akhir pengguna. Perkara yang perlu dipertimbangkan berkaitan penggunaan peranti titik akhir adalah seperti berikut: (a) apakah jenis data yang boleh diproses, disimpan atau digunakan dalam peranti titik akhir pengguna terutamanya melibatkan kategori keselamatan maklumat; (b) keperluan peranti untuk didaftarkan; (c) keperluan peranti bagi mendapat perlindungan fizikal; (d) tidak boleh membuat pemasangan perisian tanpa kebenaran; (e) pemasangan dan pengemaskinian perisian perlu mengikut peraturan semasa; (f) sambungan peranti ke talian awam atau talian luar perlu mengikut peraturan semasa; (g) kawalan capaian ke atas peranti; (h) media penyimpanan maklumat perlulah di enkripsi; (i) peranti perlu dilindungi daripada pencerobohan perisian hasad; (j) peranti boleh dihalang daripada digunakan dan data yang disimpan di dalamnya boleh dipadamkan dari jauh; (k) memastikan perancangan bagi sandaran (backup); (l) mematuhi peraturan-peraturan berkaitan penggunaan perkhidmatan dan aplikasi; (m) melaksana analisa berkaitan pengguna akhir untuk mendapatkan maklumat tentang corak interaksi pengguna dengan sistem; (n) media penyimpanan boleh tanggal seperti USB drives, boleh dimanipulasi dengan pelbagai cara. Sekiranya berlaku pelanggaran polisi, penyambungan USB perlu dinyah aktif; dan (o) keupayaan pengasingan maklumat perkhidmatan dan lain-lain maklumat boleh digunakan bagi menjaga data yang disimpan di peranti pengguna. KKM perlu melarang penyimpanan data sulit dan sensitif pada peranti titik akhir pengguna melalui kawalan teknikal.	ICTSO IPKKM ICTSO Fasiliti Pengguna
8.1.2 Tanggungjawab Pengguna Pengguna perlu dimaklumkan tentang keperluan untuk memahami prosedur, melaksana langkah keselamatan dan mematuhi polisi berkaitan penggunaan peranti titik akhir pengguna.	

8.1 PERANTI TITIK AKHIR PENGGUNA *(USER ENDPOINT DEVICES)*	PERANAN
Pengguna perlu mematuhi peraturan dan proses seperti berikut: (a) setelah perkhidmatan tidak lagi diperlukan atau sesi telah selesai, pengguna perlu log keluar dan menamatkan perkhidmatan; (b) pengguna tidak boleh meninggalkan peranti tanpa pengawasan. Apabila tidak digunakan, pegawai perlu memastikan keselamatan peranti dengan menggunakan langkah fizikal seperti mengunci dan langkah teknikal seperti kata laluan yang kukuh; (c) pengguna perlu lebih berhati-hati apabila menggunakan peranti titik akhir yang mengandungi data sulit di tempat awam yang tidak mempunyai keselamatan; dan (d) peranti titik akhir pengguna mesti dilindungi daripada kecurian, terutamanya di tempat berbahaya seperti bilik hotel, bilik mesyuarat atau transit awam.	ICTSO IPKKM ICTSO Fasiliti Pengguna
8.1.3 Penggunaan *Bring Your Own Device (BYOD)* Perkara yang perlu dipertimbangkan apabila membenarkan penggunaan peranti peribadi atau *BYOD* untuk melaksanakan tugas rasmi di KKM adalah seperti berikut: (a) memisahkan penggunaan peranti peribadi dari perkhidmatan KKM bagi melindungi maklumat KKM dengan menggunakan kaedah bersesuaian; (b) pengguna boleh mempunyai capaian kepada peranti di pejabat dengan syarat bersetuju dengan perkara berikut: (i) pengguna perlu melindungi peranti di pejabat dari segi keselamatan fizikal dan memenuhi pengemaskinian perisian keselamatan; (ii) pengguna perlu untuk tidak mengakui sebarang hak pemilikan ke atas data KKM; dan (iii) pengguna bersetuju bahawa data dalam peranti peribadi perlu dipadam jika ia hilang atau dicuri. (c) memaklumkan kepada pengguna bahawa penggunaan peranti peribadi boleh membawa implikasi undang-undang sekiranya berlaku perlanggaran ke atas polisi, dasar, arahan dan lain-lain yang sedang berkuatkuasa; dan (d) pengguna *BYOD* hendaklah memberikan persetujuan secara bertulis atau digital untuk mematuhi polisi, dasar, arahan dan lain-lain berkaitan *BYOD* yang berkuatkuasa.	ICTSO IPKKM ICTSO Fasiliti Pengguna
8.2 HAK CAPAIAN ISTIMEWA *(PRIVILEGED ACCESS RIGHTS)*	**PERANAN**
8.2.1 Pengagihan dan Penggunaan Hak Capaian Istimewa Pengagihan dan penggunaan hak capaian istimewa perlu dihadkan dan dikelola dengan sebaiknya. Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas. Hak capaian istimewa adalah seperti *Administrators Privilege, Superuser Privilege dan Root User Privilege.* (a) Menyediakan senarai pengguna yang memerlukan sebarang tahap capaian istimewa – sama ada kepada sistem individu, aplikasi atau sistem operasi; (b) Memastikan hak capaian istimewa diberikan kepada pengguna berdasarkan modul/submodul bergantung keperluan untuk melaksanakan tugas;	Pemilik Sistem

8.2 HAK CAPAIAN ISTIMEWA *(PRIVILEGED ACCESS RIGHTS)*	PERANAN
(c) Mengekalkan rekod semua hak capaian yang telah diberikan dan gariskan proses kebenaran yang jelas untuk semua permintaan capaian istimewa; (d) Memastikan hak capaian mesti tertakluk pada tarikh tamat tempoh yang ditetapkan; (e) Memaklumkan kepada pengguna secara jelas apabila beroperasi dengan menggunakan hak capaian istimewa kepada sistem; (f) Apabila diperlukan, pengguna diminta untuk membuat pengesahan semula sebelum menggunakan hak capaian istimewa bagi meningkatkan keselamatan maklumat dan data; (g) Mengaudit hak capaian istimewa secara berkala, terutamanya selepas tempoh perubahan dalam KKM. Hak capaian hendaklah disemak berdasarkan "tugas, peranan, tanggungjawab dan kecekapan" pengguna; (h) Mempertimbangkan prosedur *"break glass"* atau kecemasan, iaitu keperluan memberikan hak capaian istimewa dalam jangka masa terhad bagi memenuhi keperluan minimum untuk operasi diselesaikan (perubahan kritikal, pentadbiran sistem, dll.); (i) Memastikan semua aktiviti yang melibatkan capaian istimewa dilog; (j) Melarang penggunaan nama pengguna dan kata laluan yang standard atau sama (lihat Bab 5) untuk log masuk sistem; (k) Mengekalkan polisi menugaskan pengguna dengan identiti berasingan untuk mengawal hak capaian istimewa dengan lebih baik. Oleh itu, identiti ini boleh dikumpulkan bersama, dan diberikan pelbagai tahap capaian berdasarkan kumpulan; dan (l) Memastikan hak capaian istimewa diperuntukkan dan disimpan untuk tugas yang penting bagi memastikan rangkaian ICT berfungsi dengan baik, seperti pentadbiran dan penyelenggaraan rangkaian.	
8.3 SEKATAN CAPAIAN MAKLUMAT (INFORMATION ACCESS RESTRICTION)	**PERANAN**
8.3.1 Sekatan Capaian Maklumat Capaian kepada maklumat dan perkara berkaitan yang lain perlu dihadkan mengikut polisi kawalan capaian yang telah ditetapkan. Untuk mengekalkan kawalan yang berkesan ke atas maklumat dan aset, KKM perlu mengambil pendekatan khusus merangkumi perkara seperti berikut: (a) tidak membenarkan pengguna yang tidak berdaftar mencapai maklumat terperingkat; (b) menyediakan mekanisme konfigurasi untuk mengawal capaian kepada maklumat dalam sistem, aplikasi dan perkhidmatan; (c) mengawal data yang boleh dicapai oleh pengguna tertentu; (d) mengawal identiti atau kumpulan identiti yang mempunyai hak capaian, seperti membaca, menulis, menghapus dan melaksanakan (execute);	Pemilik Sistem

8.2 HAK CAPAIAN ISTIMEWA *(PRIVILEGED ACCESS RIGHTS)*	PERANAN
(e) menyediakan kawalan capaian fizikal atau logikal untuk mengasingkan aplikasi sensitif, data aplikasi, atau sistem; dan (f) pentadbir Sistem hendaklah melaksanakan semakan dan pemantauan secara berkala sekurang-kurangnya setahun sekali bagi memastikan pengguna yang mencapai sistem adalah sah.	
8.3.2 Pengurusan Capaian Dinamik Pengurusan Capaian Dinamik merujuk kepada pendekatan pengurusan capaian yang membolehkan penyesuaian dan perubahan hak capaian pengguna secara real-time atau berdasarkan keadaan tertentu. Berbeza dengan pengurusan capaian tradisional yang statik, pengurusan capaian dinamik menyesuaikan capaian berdasarkan faktor-faktor seperti konteks, lokasi, masa, keadaan sistem, atau atribut pengguna. Perkara yang boleh dipertimbangkan apabila menggunakan pendekatan pengurusan Capaian Dinamik adalah seperti berikut: (a) Konteks dan Keadaan: Hak capaian boleh berubah mengikut konteks seperti lokasi fizikal, masa, atau status keselamatan sistem; (b) Fleksibiliti dan Penyesuaian: Sistem ini membolehkan penyesuaian hak capaian dengan lebih fleksibel mengikut keperluan semasa; (c) Keputusan Capaian Berdasarkan Data Masa Nyata: Capaian boleh diberikan atau ditolak berdasarkan keadaan semasa, contohnya, jika seorang pengguna mencapai sistem dari lokasi yang tidak biasa atau pada waktu yang luar biasa; dan (d) Peningkatan Keselamatan: Dengan membolehkan perubahan capaian secara dinamik, ia membantu mengurangkan risiko dan meningkatkan keselamatan sistem. Contoh: Seorang pengguna mungkin mempunyai capaian penuh pada waktu pejabat, tetapi capaiannya dihadkan atau dihentikan jika cuba mencapai sistem di luar waktu pejabat atau dari lokasi yang tidak dikenali.	Pentadbir Sistem ICT Pemilik Sistem
8.3.3 Kawalan ke atas Percubaan Capaian Kawalan perlu diberikan ke atas semua percubaan capaian bagi memastikan data dilindungi dengan mempertimbangkan perkara berikut: (a) memastikan capaian diberikan berdasarkan pengesahan yang berjaya; (b) menyediakan tahap capaian terhad bergantung kepada pengelasan data; (c) mengawal kebenaran cetakan; (d) melaksana enkripsi; dan (e) menyimpan log audit komprehensif yang merekodkan siapa yang mencapai data dan tujuan penggunaan data. Prosedur makluman yang memberi amaran, sebarang penggunaan data yang tidak wajar termasuk (walaupun tidak terhad kepada) tiada kebenaran capaian, pengedaran dan percubaan untuk menghapusnya.	Pentadbir Sistem ICT Pemilik Sistem

8.4 CAPAIAN KEPADA KOD SUMBER *(ACCESS TO SOURCE CODE)*	PERANAN
8.4.1 Capaian kepada Kod Sumber Capaian kepada kepada kod sumber perlu dikelola dengan sewajarnya. KKM perlu mentadbir capaian dan pindaan kepada kod sumber secara berpusat di seluruh lokasi ICT dengan sistem pengurusan kod sumber. KKM digalakkan mempertimbangkan capaian yang selamat kepada kod sumber mengikut keistimewaan untuk membaca/menulis berdasarkan kategori kod sumber, dari mana ia dicapai dan siapa yang mencapainya. Perkara yang perlu dipertimbangkan dalam mengawal capaian kod sumber adalah seperti berikut: (a) Memastikan capaian kepada kos sumber berdasarkan keperluan perkhidmatan yang ditentukan secara *case-by-case* atau *user-by-user;* (b) Apabila mentadbir capaian kepada kod sumber, KKM perlu mengikut satu set prosedur pengurusan perubahan (rujuk Bab 8); (c) Memastikan semua aktiviti berkaitan kod sumber termasuk timestamp dan aktiviti berkaitan perubahan, perlu dikekalkan dalam jejak audit secara bersama; dan (d) Memberi capaian baca dan tulis kepada kod sumber berdasarkan keperluan dan berupaya mengawal risiko mengubah atau menyalah guna kod sumber.	Pentadbir Sistem ICT Pemilik Sistem Pihak Ketiga
8.5 PENGESAHAN SELAMAT *(SECURE AUTHENTICATION)*	**PERANAN**
8.5.1 Pengesahan Yang Selamat KKM perlu mengambil kira pengelasan data dan rangkaian yang dicapai apabila mempertimbangkan kawalan pengesahan yang ingin dilaksanakan. Contoh kawalan tersebut termasuk: (a) kawalan capaian pintar (kad pintar); (b) log masuk biometrik. (c) token selamat *(Secure tokens);* (d) pengesahan pelbagai faktor *(Multi factor authentication);* dan (e) sijil digital. Matlamat utama pengesahan yang selamat adalah untuk menghalang dan mengurangkan kemungkinan capaian tanpa kebenaran kepada sistem yang dilindungi. Perkara yang perlu dipertimbangkan dalam kawalan ini adalah seperti berikut: (a) memastikan maklumat hanya dipaparkan selepas proses pengesahan berjaya; (b) menunjukkan mesej amaran sebelum log masuk yang menyatakan dengan jelas hanya pengguna yang dibenarkan boleh mencapai data; (c) mengurangkan bantuan yang diberi kepada pengguna yang tidak/ belum dibenarkan masuk ke dalam sistem. Sebagai contoh: (i) sistem tidak sepatutnya mendedahkan bahagian/ruang log masuk yang salah seperti memfokuskan kesilapan pada ruang kata laluan; atau	Pemilik Sistem Pentadbir Sistem ICT

8.5 PENGESAHAN SELAMAT *(SECURE AUTHENTICATION)*	PERANAN
(i) sistem tidak sepatutnya mendedahkan bahagian/ruang log masuk yang salah seperti memfokuskan kesilapan pada ruang kata laluan; atau (ii) tidak memaklumkan kesilapan sebagai sebahagian proses pengesahan, sebaliknya, hanya memaklumkan bahawa log masuk tidak berjaya. (d) mengesahkan percubaan log masuk hanya apabila semua maklumat yang diperlukan telah dibekalkan kepada servis log masuk; (e) melaksanakan langkah keselamatan berdasarkan piawaian industri untuk melindungi daripada capaian menyeluruh *(blanket access)* dan serangan "cuba dan gagal" *(brute force attack)* pada servis log masuk. Perkara yang boleh dipertimbangan dilaksanakan dan tidak terhad kepada perkara berikut: (i) CAPTCHA ialah ciri keselamatan yang diperlukan untuk mengesahkan bahawa anda adalah pengguna manusia; (ii) menguatkuasakan penetapan semula kata laluan berikutan bilangan percubaan log masuk yang tidak berjaya; dan (iii) selepas beberapa percubaan yang tidak berjaya, log masuk selanjutnya perlu digagalkan. Perkara ini boleh diadakan dengan menetapkan had percubaan maksimum 3 kali. (f) untuk pengauditan dan keselamatan, setiap percubaan log masuk yang gagal hendaklah diberi perhatian dan direkodkan; (g) sekiranya berlaku sebarang percanggahan log masuk, seperti pencerobohan yang disyaki, prosedur pengendalian insiden keselamatan mesti dimulakan dengan segera. Pegawai dalaman, terutamanya yang mempunyai capaian pentadbir sistem atau keupayaan untuk menghalang percubaan log masuk berniat jahat, perlu dimaklumkan dengan segera; (h) merekod waktu log masuk terakhir yang berlaku dengan mencatat tarikh dan masa; (i) merekod semua percubaan log masuk sejak log masuk terakhir yang disahkan; (j) menetapkan kata laluan sebagai asterisk atau simbol abstrak lain yang serupa, melainkan ada sebab untuk ditunjukkan (Contoh: kebolehcapaian *(accessibility)* pengguna); (k) tiada toleransi ke atas kata laluan yang dikongsi atau dipaparkan dalam teks biasa yang boleh dibaca; (l) memastikan sesi log masuk yang melahu (idle) ditamatkan selepas jangka masa yang ditetapkan terutama untuk sesi yang berisiko tinggi (situasi kerja dari jauh) atau pada peranti milik pengguna (BYOD), seperti komputer riba atau telefon mudah alih; dan (m) menghadkan tempoh sesi yang telah disahkan, walaupun semasa aktif, bergantung pada data yang dicapai (Contoh: maklumat perkhidmatan penting atau program berkaitan kewangan).	

8.5 PENGESAHAN SELAMAT *(SECURE AUTHENTICATION)*	PERANAN
Disarankan proses log masuk biometrik digabungkan dengan sekurang-kurangnya satu teknik log masuk yang lain, kerana lebih berkesan dan berintegriti jika dibandingkan dengan kaedah tradisional seperti kata laluan, Multi-Factor Authentication (MFA) dan token.	
8.6 PENGURUSAN KAPASITI *(CAPACITY MANAGEMENT)*	**PERANAN**
8.6.1 Pengurusan Kapasiti Penggunaan sumber perlu dipantau dan diselaraskan mengikut keperluan kapasiti semasa atau berdasarkan kepada unjuran bagi memastikan sistem dalam keadaan yang terbaik. Perkara yang perlu dipatuhi berkaitan pengurusan kapasiti adalah seperti berikut: (a) 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; (b) Kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang; dan (c) Mempertingkatkan penggunaan pengkomputeran awan bagi pengurusan kapasiti yang berkesan, anjal *(elasticity)* dan boleh skala *(scalability)*.	Pemilik Sistem Pegawai Kejuruteraan Pentadbir Sistem ICT
8.6.2 Pengurusan Permintaan Kapasiti Kawalan ini adalah berkaitan pengurusan kapasiti – sama ada menambah kapasiti atau mengurangkan permintaan daripada pengguna. Perkara yang boleh dipertimbangkan apabila terdapat keperluan untuk menambah kapasiti adalah seperti berikut: (a) membawa pegawai baharu untuk melaksanakan tugas kerja; (b) mendapatkan kemudahan atau ruang pejabat baharu melalui pembelian, pajakan atau penyewaan; (c) mendapatkan pemprosesan tambahan, storan data dan *Random Access Memory* (RAM) (di tapak atau berasaskan awan) sama ada melalui pembelian, pajakan atau penyewaan; (d) menimbang untuk menggunakan sumber awan 'anjal *(elastic)*' dan 'berskala *(scalable)*' yang berkembang mengikut keperluan pemprosesan perkhidmatan sehingga hampir tiada penglibatan. Perkara yang dipertimbangkan untuk mengurangkan permintaan kepada penambahan kapasiti adalah seperti berikut: (a) menghapuskan maklumat lapuk untuk membersihkan kapasiti storan pada pelayan dan media yang berkaitan; (b) menghapuskan dengan selamat sebarang salinan cetak maklumat yang tidak diperlukan oleh KKM dan tidak diberi mandat untuk disimpan melalui perundangan atau peraturan; (c) menghentikan penggunaan sebarang sumber ICT, aplikasi atau tetapan maya yang tidak diperlukan lagi;	Pemilik Sistem Pentadbir Sistem ICT

8.6 PENGURUSAN KAPASITI *(CAPACITY MANAGEMENT)*	PERANAN
(d) memeriksa aktiviti ICT (termasuk akaun, penyelenggaraan automatik dan aktiviti kelompok) untuk memaksimumkan keupayaan memori dan dapat memberi ruang yang lebih besar; (e) memaksimumkan kod aplikasi dan kuiri pangkalan data yang cukup kerap berlaku untuk meningkatkan keupayaan operasi perkhidmatan; dan (f) menghadkan jumlah jalur lebar yang diperuntukkan kepada aktiviti yang tidak penting pada rangkaian perkhidmatan. Ini termasuk menyekat capaian Internet dan menyekat penstriman video/audio daripada peranti kerja.	
8.7 PERLINDUNGAN TERHADAP PERISIAN HASAD *(PROTECTION AGAINST MALWARE)*	**PERANAN**
8.7.1 Perlindungan terhadap Perisian Hasad Perlindungan terhadap perisian hasad perlu dilaksanakan dan hanya akan berkesan sekiranya program kesedaran kepada pengguna berkaitan kepentingan untuk melindungi sistem perkhidmatan dari perisian hasad dilaksanakan dengan berkesan. Kawalan ini memerlukan KKM untuk melaksanakan perlindungan dari perisian hasad yang merangkumi empat aspek utama: (a) sistem terkawal dan capaian akaun; (b) pengurusan perubahan; (c) perisian *anti-malware;* dan (d) kesedaran keselamatan maklumat KKM (latihan pengguna). Penggunaan perisian anti-malware adalah tidak mencukupi untuk memberikan kawalan keselamatan terhadap perisian hasad. KKM perlu menggunakan strategi hujung ke hujung *(end-to-end)* terhadap perisian hasad, yang bermula dengan mendidik pengguna dan mengutamakan penggunaan rangkaian selamat seterusnya meminimumkan kemungkinan pencerobohan daripada pelbagai sumber serangan. Perkara yang perlu dipertimbangkan untuk dilaksanakan dalam melindungi sistem perkhidmatan dari perisian hasad adalah seperti berikut: (a) tidak menggalakkan penggunaan perisian yang tidak diluluskan; (b) menutup capaian kepada laman sesawang berniat jahat atau tidak sesuai; (c) mengurangkan bilangan kerentanan yang wujud pada rangkaian yang boleh dimanipulasi oleh perisian hasad atau individu dengan niat jahat; (d) melaksanakan pengesanan perisian hasad dengan imbasan tetap dan menyeluruh ke atas semua sistem dan fail; (e) pegawai teknikal diberi kebenaran untuk menyahaktifkan beberapa atau semua perisian anti-hasad apabila ia mengganggu operasi KKM; (f) melaksanakan BUDR bagi membolehkan KKM beroperasi semula selepas gangguan (rujuk Bab 8);	Pemilik Sistem Pentadbir Sistem ICT

8.7 PERLINDUNGAN TERHADAP PERISIAN HASAD *(PROTECTION AGAINST MALWARE)*	PERANAN
(g) melaksana segmentasi ke atas rangkaian dan/atau ruang kerja digital dan maya kepada beberapa bahagian untuk mengelakkan kerosakan besar sekiranya serangan berlaku; (h) memberikan latihan kepada pegawai berkaitan perisian anti-hasad untuk meningkatkan pemahaman tentang keselamatan siber, termasuk (tetapi tidak terhad kepada); (i) keselamatan e-mel; (ii) pemasangan perisian hasad; dan (ii) kejuruteraan sosial (social engineering). (i) memastikan semua pemberitahuan mengenai kemungkinan serangan perisian hasad (terutamanya daripada pihak ketiga perisian dan perkakasan) datang daripada sumber yang boleh dipercayai dan tepat.	
8.8 PENGURUSAN KERENTANAN TEKNIKAL *(MANAGEMENT OF TECHNICAL VULNERABILITIES)*	**PERANAN**
8.8.1 Pengurusan Kerentatan Teknikal Maklumat mengenai kerentanan teknikal sistem maklumat yang digunakan perlu diperoleh. Maklumat berkaitan kerentanan tersebut perlu dinilai, dan langkah-langkah yang sesuai perlu diambil. Sebelum melaksanakan kawalan kerentanan adalah penting untuk memperoleh senarai aset fizikal dan digital yang komprehensif dan terkini (rujuk Bab 5) yang dimiliki dan dikendalikan oleh KKM. KKM perlu berusaha untuk mengenal pasti kelemahan teknikal dengan: (a) mengenal pasti siapa yang bertanggungjawab ke atas perisian; (b) menyimpan rekod aplikasi dan alatan untuk mengenal pasti kelemahan teknikal; (c) meminta pihak ketiga mendedahkan berkaitan sebarang kerentanan pada sistem dan perkakasan baharu apabila membekalkannya (seperti Bab 5), dan perlu dinyatakan dengan jelas dalam kontrak dan perjanjian perkhidmatan; (d) menggunakan alat pengimbasan kerentanan dan kemudahan menampal (patching); (e) melakukan ujian penembusan berkala yang didokumenkan sama ada oleh pegawai dalaman atau oleh pihak ketiga yang disahkan; (f) berhati-hati tentang potensi kerentanan pada program yang dipasang apabila menggunakan repositori kod pihak ketiga atau kod sumber; dan (g) mengemas kini kelemahan (vulnerabilities) secara berkala bagi kesemua aset ICT yang berkemungkinan mempengaruhi vektor dan eksploitasi serangan yang akan berlaku. KKM perlu menyemak sebarang tindakan pembetulan yang diambil dan mempertimbangkan untuk berkongsi maklumat berkaitan kepada individu atau jabatan yang terjejas. Selain itu, KKM perlu melibatkan diri dengan organisasi pakar keselamatan untuk berkongsi pengetahuan tentang kerentanan dan vektor serangan.	Pemilik Sistem Pentadbir Sistem ICT

8.8 PENGURUSAN KERENTANAN TEKNIKAL *(MANAGEMENT OF TECHNICAL VULNERABILITIES)*	PERANAN
8.8.2 Menilai Kerentanan Pelaporan yang tepat adalah penting untuk memastikan tindakan pembetulan yang cepat dan berkesan apabila risiko keselamatan dikesan. KKM perlu menilai kerentanan dengan: (a) memeriksa laporan dengan teliti dan tentukan tindakan yang perlu, seperti menukar, mengemas kini atau menghapuskan sistem dan/atau peralatan yang terjejas; dan (b) mencapai resolusi dengan mengambil kira kawalan lain (terutamanya yang berkaitan) dan mengakui tahap risiko.	Pemilik Sistem Pentadbir Sistem ICT
8.8.3 Menangani Kelemahan Perisian Kerentanan perisian boleh diatasi dengan menggunakan pendekatan proaktif untuk mengemas kini perisian dan mengurus tampalan (patching). Memastikan kemas kini dan tampalan tetap boleh membantu melindungi sistem KKM daripada kemungkinan ancaman. Setelah kerentanan dikenal pasti, KKM perlu mengambil tindakan seperti berikut: (a) memperbaiki semua kelemahan keselamatan dengan pantas dan berkesan; (b) mematuhi prosedur KKM dalam Pengurusan Perubahan (lihat Bab 8) dan Pengendalian Insiden (rujuk Bab 5); (c) hanya menggunakan tampalan dan kemas kini daripada sumber yang boleh dipercayai dan diperakui, terutamanya untuk perisian dan peralatan pihak ketiga; (d) sebelum memasang, atau mengemas kini, ujian perlu dilaksanakan untuk mengelakkan sebarang masalah yang tidak dijangka; (e) memberi keutamaan untuk menangani sistem perkhidmatan yang berisiko tinggi dan penting; dan (f) memastikan tindakan pemulihan berjaya dan berkualiti. Sekiranya tiada kemas kini tersedia atau terdapat sebarang halangan untuk memasangnya (Contoh: melibatkan kos), KKM perlu memikirkan kaedah lain. Perkara yang boleh dipertimbangkan adalah seperti berikut: (a) meminta panduan daripada pihak ketiga mengenai pembaikan sementara, sementara usaha pembaikan utama dipergiatkan; (b) mematikan sebarang perkhidmatan rangkaian yang terjejas oleh kerentanan; (c) melaksanakan kawalan keselamatan di pintu masuk *(gateway)* untuk melindungi rangkaian; (d) meningkatkan pengawasan mengikut kadar risiko yang berkaitan; (e) memastikan semua pihak yang berkenaan menyedari kerentanan, termasuk pihak ketiga dan pembeli/pemilik; dan (f) menangguhkan kemas kini dan menilai risiko, terutamanya melibatkan sebarang kos operasi.	Pemilik Sistem Pentadbir Sistem ICT

8.8 PENGURUSAN KERENTANAN TEKNIKAL *(MANAGEMENT OF TECHNICAL VULNERABILITIES)*	PERANAN
8.8.4 Panduan Sokongan KKM perlu mengekalkan jejak audit semua aktiviti pengurusan kerentanan yang berkaitan untuk membantu tindakan pembetulan dan bagi melaksana prosedur awal sekiranya berlaku pelanggaran keselamatan. Menilai dan menyemak keseluruhan proses pengurusan kerentanan secara berkala ialah cara terbaik untuk meningkatkan prestasi dan mengenal pasti sebarang kelemahan secara proaktif. Jika KKM menggunakan penyedia perkhidmatan awan, KKM perlu memastikan pendekatan pihak ketiga terhadap pengurusan kelemahan mereka sesuai dan dapat digunakan dalam perkhidmatan mereka sendiri serta perlu disertakan dalam perjanjian perkhidmatan yang mengikat antara kedua-dua pihak termasuk sebarang prosedur pelaporan (lihat Bab 5).	Pemilik Sistem Pentadbir Sistem ICT
8.9 PENGURUSAN KONFIGURASI *(CONFIGURATION MANAGEMENT)*	**PERANAN**
8.9.1 Pengurusan Konfigurasi Pengurusan konfigurasi perlu dirangka dan digubal untuk kedua-dua sistem baharu dan sedia ada serta perkakasan. Kawalan dalaman hendaklah diwujudkan merangkumi elemen utama seperti konfigurasi keselamatan, perkakasan dengan fail konfigurasi dan sebarang perisian atau sistem yang berkenaan. KKM perlu mempertimbangkan semua peranan dan tugas yang berkaitan apabila mewujudkan dasar konfigurasi, termasuk memberikan pemilikan konfigurasi berdasarkan peranti demi peranti atau aplikasi demi aplikasi.	Pentadbir Server Pentadbir Sistem ICT Pentadbir Rangkaian
8.9.2 Panduan terhadap Kawalan Keselamatan Konfigurasi Perkara yang perlu dipertimbangkan untuk mengurangkan potensi bahaya keselamatan maklumat dengan: (a) menghadkan jumlah pegawai yang mempunyai kuasa pentadbiran kepada kuantiti yang paling sedikit; (b) menyahaktifkan sebarang identiti yang tidak digunakan atau tidak diperlukan; (c) menjejaki capaian kepada program penyelenggaraan utiliti dan tetapan dalaman dengan berhati-hati; (d) memastikan masa diselaraskan untuk merekodkan konfigurasi dengan tepat dan membantu sebarang pemeriksaan masa hadapan; (e) menukar terus mana-mana kata laluan lalai (default password) atau tetapan keselamatan yang disediakan dengan mana-mana peranti perkhidmatan atau program; (f) melaksanakan tempoh log keluar untuk mana-mana peranti, sistem atau aplikasi yang tidak aktif untuk jangka masa yang telah ditetapkan; dan (g) memastikan pematuhan Kawalan Hak Harta Intelek untuk menjamin bahawa semua keperluan pelesenan telah dipenuhi.	Pentadbir Server Pentadbir Sistem ICT
8.9.3 Panduan Mengurus dan Memantau Konfigurasi KKM bertanggungjawab untuk mengekalkan dan merekodkan sebarang perubahan konfigurasi selaras dengan proses Pengurusan Perubahan Bab 8.	Pentadbir Server Pentadbir Sistem ICT Pentadbir Rangkaian

8.9 PENGURUSAN KONFIGURASI *(CONFIGURATION MANAGEMENT)*	PERANAN
KKM perlu menggunakan perisian khusus untuk memantau sebarang perubahan pada konfigurasi peranti, mengambil tindakan pantas sama ada untuk meluluskan atau mengembalikan perubahan konfigurasi kepada status asalnya.	
8.10 PENGHAPUSAN MAKLUMAT *(INFORMATION DELETION)*	**PERANAN**
8.10.1 Penghapusan Maklumat Maklumat yang disimpan dalam sistem, peranti atau dalam media penyimpanan lain perlu dihapuskan apabila tidak lagi diperlukan. Menghapuskan data apabila ia tidak diperlukan untuk mengurangkan risiko pendedahan kepada mereka yang tidak diberi kuasa untuk mencapainya. Perkara yang boleh dipertimbangkan dalam penghapusan maklumat adalah seperti berikut: (a) memilih kaedah penghapusan yang sesuai yang mematuhi arahan, peraturan, pekeliling yang sedang berkuatkuasa ; (b) merekodkan hasil penghapusan untuk rujukan masa hadapan; (c) memastikan bahawa, apabila menggunakan sanitasi pihak ketiga, KKM memperoleh bukti yang mencukupi (biasanya melalui dokumentasi) bahawa proses sanitasi telah dilakukan; dan (d) menyatakan dengan tepat senarai keperluan pihak ketiga, termasuk kaedah penghapusan dan jangka masa, dan perlu menjamin bahawa aktiviti sanitasi disertakan dalam kontrak yang mengikat kedua-dua pihak.	Pegawai Aset Pemilik Sistem Pemilik Aset
8.11 PENYAMARAN DATA *(DATA MASKING)*	**PERANAN**
8.11.1 Penyamaran Data Penyamaran data perlu digunakan mengikut polisi, arahan, pekeliling, garis panduan yang sedang berkuatkuasa sekiranya ada. Kawalan ini memboleh data disembunyikan melalui dua teknik utama - nama samaran *(pseudonymisation)* dan/atau tanpa nama *(anonymisation)*. Teknik ini bertujuan untuk menyembunyikan tujuan sebenar PII dengan memutuskan hubungan antara data mentah (raw data) dengan subjek (kebiasaannya seseorang).	Pemilik Sistem Pentadbir Sistem ICT
8.11.2 Teknik yang boleh digunakan Perkara yang boleh dipertimbangkan untuk diguna pakai bagi meningkatkan keselamatan data: (a) penyulitan menggunakan kekunci; (b) penghapusan atau pengeluaran aksara dari set data; (c) variasikan nombor dan tarikh yang digunakan; (d) menggantikan nilai di keseluruhan data; dan (e) penyamaran secara *hash-based.*	Pemilik Sistem Pentadbir Sistem ICT

8.11 PENYAMARAN DATA *(DATA MASKING)*	PERANAN
8.11.3 Panduan mengenai Prinsip Penyamaran Data Penyamaran data ialah elemen penting untuk melindungi PII dan bagi menjamin kerahsiaan data yang disimpan. Perkara yang perlu diambil kira dalam strategi penyamaran data adalah seperti berikut: (a) melaksanakan teknik penyamaran untuk mendedahkan hanya sedikit mungkin jumlah data kepada pengguna; (b) cebisan data tertentu disembunyikan (dikaburkan) dan capaian pegawai pada bahagian yang berkaitan adalah terhad kepada ahli tertentu sahaja; (c) membina prosedur penyamaran data mengikut keperluan undang-undang dan peraturan; dan (d) *Pseudonymisation* memerlukan penggunaan algoritma untuk membuka penyamaran data dan mesti disimpan dengan selamat.	Pemilik Sistem Pentadbir Sistem ICT
8.12 PENCEGAHAN KEBOCORAN DATA *(DATA LEAKAGE PREVENTION)*	**PERANAN**
8.12.1 Pencegahan Kebocoran Data Langkah-langkah pencegahan kebocoran data perlu dilaksanakan pada rangkaian dan peranti lain yang memproses, menyimpan atau menghantar maklumat. Perkara yang perlu dipatuhi bagi mengurangkan risiko kebocoran data adalah seperti berikut: (a) menyusun data mengikut piawaian industri (PII, data komersial, maklumat produk) untuk menetapkan tahap risiko yang berbeza; (b) memeriksa dengan teliti saluran data yang banyak digunakan dan boleh berlaku kebocoran (Contoh: e-mel, pemindahan fail ke dalam dan ke luar, alat USB); (c) mengambil langkah proaktif dalam melindungi data daripada terdedah.; (d) menghadkan kapasiti pengguna untuk menyalin *(copy)* dan menampal *(paste)* data (jika berkenaan) hanya kepada/dari platform dan sistem tertentu; (e) memastikan kebenaran diperolehi daripada pemilik data sebelum sebarang eksport data; (f) mengawal selia atau menghentikan pengguna daripada menangkap tangkapan skrin atau mengambil gambar monitor yang menunjukkan jenis data yang dilindungi; (g) menyulitkan *(encrypted)* sebarang sandaran yang mempunyai data sensitif; dan (h) membina langkah-langkah keselamatan pintu masuk (gateway) dan pencegahan kebocoran untuk melindungi daripada pengaruh luar, termasuk (tetapi tidak terhad kepada) pengintipan industri, sabotaj, gangguan komersial dan kecurian harta intelek (Intellectual Property). Pencegahan kebocoran data berkait rapat dengan garis panduan keselamatan lain yang bertujuan untuk melindungi maklumat dan data di seluruh rangkaian KKM, termasuk kawalan capaian dan pengurusan dokumen yang selamat.	Pemilik Sistem Pentadbir Sistem ICT

8.13 SANDARAN MAKLUMAT *(INFORMATION BACKUP)*	PERANAN
8.13.1 Sandaran Maklumat Salinan sandaran bagi maklumat, perisian dan sistem perlu dikekalkan dan diuji secara berkala mengikut prosedur sandaran yang telah dipersetujui. Semua data perkhidmatan-kritikal, perisian dan sistem perlu mempunyai kemudahan sandaran untuk memastikan ia boleh dipulihkan sekiranya berlaku perkara seperti di bawah: (a) gangguan perkhidmatan; (b) kegagalan sistem, aplikasi atau media penyimpanan; (c) kehilangan data; (d) pencerobohan; Perkara yang perlu dipertimbangan dalam merangka Pelan Sandaran adalah seperti berikut: (a) mengenal pasti semua sistem dan perkhidmatan kritikal dan menggariskan prosedur pemulihan yang jelas dan ringkas; (b) memastikan keperluan operasi KKM dipenuhi (Contoh: objektif masa pemulihan, jenis sandaran, kekerapan sandaran); (c) mengekalkan sandaran di lokasi yang sesuai berasingan secara fizikal daripada data sumber dan boleh dicapai dengan selamat untuk penyelenggaraan; (d) memastikan ketersediaan data apabila berlaku gangguan dan kekerapan ujian ke atas sandaran adalah penting; (e) masa pemulihan perlu dipersetujui dan perlu diukur berdasarkan ujian sandaran untuk memastikan ia mematuhinya sekiranya berlaku kehilangan data atau kegagalan sistem; (f) memastikan data yang telah disandarkan hendaklah disulitkan mengikut tahap pengelasan; (g) memastikan kehilangan data diperiksa terlebih dahulu sebelum sebarang kerja sandaran dijalankan; (h) memastikan pegawai penyelenggaraan dimaklumkan tentang status kerja sandaran supaya tindakan pembaikan boleh diambil jika mereka gagal sepenuhnya atau sebahagiannya; (i) memastikan data daripada platform berasaskan awan yang tidak diuruskan secara langsung oleh KKM perlu disertakan dalam sandaran; dan (j) memastikan data sandaran disimpan mengikut polisi sandaran yang ditetapkan termasuk pemindahan dan/atau pengarkiban ke media storan.	Pentadbir Sistem ICT
8.14 LEWAHAN FASILITI PEMPROSESAN MAKLUMAT *(REDUNDANCY OF INFORMATION PROCESSING FACILITIES)*	**PERANAN**
8.14.1 Lewahan Fasiliti Pemprosesan Maklumat KKM perlu mengenal pasti keperluan, mereka bentuk dan melaksanakan lewahan untuk memastikan kesinambungan perkhidmatan dan ketersediaan kemudahan pemprosesan maklumat.	Pentadbir Pusat Data Pemilik Sistem Pentadbir Sistem ICT Pegawai Kejuruteraan

8.13 SANDARAN MAKLUMAT *(INFORMATION BACKUP)*	PERANAN
8.13.1 Sandaran Maklumat Salinan sandaran bagi maklumat, perisian dan sistem perlu dikekalkan dan diuji secara berkala mengikut prosedur sandaran yang telah dipersetujui. Semua data perkhidmatan-kritikal, perisian dan sistem perlu mempunyai kemudahan sandaran untuk memastikan ia boleh dipulihkan sekiranya berlaku perkara seperti di bawah: (a) gangguan perkhidmatan; (b) kegagalan sistem, aplikasi atau media penyimpanan; (c) kehilangan data; (d) pencerobohan; Perkara yang perlu dipertimbangan dalam merangka Pelan Sandaran adalah seperti berikut: (a) mengenal pasti semua sistem dan perkhidmatan kritikal dan menggariskan prosedur pemulihan yang jelas dan ringkas; (b) memastikan keperluan operasi KKM dipenuhi (Contoh: objektif masa pemulihan, jenis sandaran, kekerapan sandaran); (c) mengekalkan sandaran di lokasi yang sesuai berasingan secara fizikal daripada data sumber dan boleh dicapai dengan selamat untuk penyelenggaraan; (d) memastikan ketersediaan data apabila berlaku gangguan dan kekerapan ujian ke atas sandaran adalah penting; (e) masa pemulihan perlu dipersetujui dan perlu diukur berdasarkan ujian sandaran untuk memastikan ia mematuhinya sekiranya berlaku kehilangan data atau kegagalan sistem; (f) memastikan data yang telah disandarkan hendaklah disulitkan mengikut tahap pengelasan; (g) memastikan kehilangan data diperiksa terlebih dahulu sebelum sebarang kerja sandaran dijalankan; (h) memastikan pegawai penyelenggaraan dimaklumkan tentang status kerja sandaran supaya tindakan pembaikan boleh diambil jika mereka gagal sepenuhnya atau sebahagiannya; (i) memastikan data daripada platform berasaskan awan yang tidak diuruskan secara langsung oleh KKM perlu disertakan dalam sandaran; dan (j) memastikan data sandaran disimpan mengikut polisi sandaran yang ditetapkan termasuk pemindahan dan/atau pengarkiban ke media storan.	Pentadbir Sistem ICT
8.14 LEWAHAN FASILITI PEMPROSESAN MAKLUMAT *(REDUNDANCY OF INFORMATION PROCESSING FACILITIES)*	**PERANAN**
8.14.1 Lewahan Fasiliti Pemprosesan Maklumat KKM perlu mengenal pasti keperluan, mereka bentuk dan melaksanakan lewahan untuk memastikan kesinambungan perkhidmatan dan ketersediaan kemudahan pemprosesan maklumat.	Pentadbir Pusat Data Pemilik Sistem Pentadbir Sistem ICT Pegawai Kejuruteraan

8.14 LEWAHAN FASILITI PEMPROSESAN MAKLUMAT *(REDUNDANCY OF INFORMATION PROCESSING FACILITIES)*	PERANAN
8.14.1 Lewahan Fasiliti Pemprosesan Maklumat KKM perlu mengenal pasti keperluan, mereka bentuk dan melaksanakan lewahan untuk memastikan kesinambungan perkhidmatan dan ketersediaan kemudahan pemprosesan maklumat. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) mengenal pasti keperluan dan tahap kritikal bagi ketersediaan perkhidmatan dan sistem maklumat; (b) menyediakan lewahan bagi kemudahan pemprosesan maklumat yang dikenal pasti; (c) menguji keberkesanan *(failover testing)* untuk memastikan keberkesanan kemudahan lewahan secara berkala; dan (d) menyediakan mekanisme yang bersesuaian untuk memberi amaran gangguan atau kegagalan kemudahan pemprosesan maklumat kepada pemilik sistem untuk memastikan lewahan tersebut boleh mengambil alih fungsi kemudahan utama semasa ianya dibaiki atau diganti.	Pentadbir Pusat Data Pemilik Sistem Pentadbir Sistem ICT Pegawai Kejuruteraan
8.15 LOG *(LOGGING)*	**PERANAN**
8.15.1 Penyediaan Log Sistem yang dibangunkan perlu merekod aktiviti dan menjana bahan bukti untuk memastikan maklumat log adalah berintegriti dan boleh digunakan sebagai bahan bukti jika berlaku insiden keselamatan maklumat. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) menyedia, menyimpan, melindungi dan menganalisis log yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa berkaitan keselamatan maklumat. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem; (b) log hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan; dan (c) log hendaklah disimpan dan direkodkan selaras dengan arahan/ pekeliling yang sedang berkuatkuasa. Log hendaklah dikawal bagi mengekalkan integriti data. Jenis fail log bagi pelayan dan aplikasi yang perlu diaktifkan ialah seperti yang berikut: (i) Fail log sistem pengoperasian; (ii) Fail log perkhidmatan (service) (contoh: web, e-mel); (iii) Fail log aplikasi (audit trail); dan (iv) Fail log rangkaian (contoh: switch, firewall, IPS).	Pentadbir Sistem ICT CSIRT IPKKM CSIRT Fasiliti KKM
8.15.3 Panduan Analisa Log Analisis log adalah sangat penting dalam usaha untuk mengenal pasti insiden keselamatan siber bagi tujuan untuk mencegah pengulangan insiden daripada berulang.	Pentadbir Sistem ICT CSIRT IPKKM CSIRT Fasiliti KKM

8.15 LOG *(LOGGING)*	PERANAN
8.15.3 Panduan Analisa Log Analisis log adalah sangat penting dalam usaha untuk mengenal pasti insiden keselamatan siber bagi tujuan untuk mencegah pengulangan insiden daripada berulang. Perkara yang perlu dipertimbangkan dalam menganalisa log adalah seperti berikut: (a) pegawai yang menjalankan analisa perlu mempunyai tahap kepakaran yang sesuai; (b) log dianalisis mengikut prosedur yang sedang berkuatkuasa; (c) peristiwa yang akan dianalisa mesti dikategorikan dan dikenal pasti mengikut jenis dan sifat;dan (d) membuat analisa keadaan trafik rangkaian yang biasa berbanding keadaan trafik yang tidak normal/luar biasa.	Pentadbir Sistem ICT CSIRT IPKKM CSIRT Fasiliti KKM
8.15.4 Pemantauan Log Perkara yang perlu dipertimbangkan semasa melaksana pemantauan log adalah seperti berikut: (a) semak sebarang percubaan capaian ke atas sumber terkawal dan perkhidmatan-kritikal seperti pelayan domain, laman portal dan platform perkongsian fail; (b) periksa rekod Domain Name System (DNS) untuk mengenal pasti sebarang trafik keluar yang mencurigakan; (c) mengumpul rekod penggunaan data daripada pihak ketiga perkhidmatan atau sistem dalaman untuk mengenali sebarang bentuk aktiviti yang luar biasa; dan (d) kumpulkan rekod dari pintu masuk fizikal, seperti log kad kunci/fob dan data capaian bilik. KKM perlu mempertimbangkan penggunaan program utiliti khas untuk menyaring sejumlah besar maklumat yang dihasilkan oleh log sistem, sekali gus menjimatkan masa dan sumber semasa menyiasat insiden keselamatan, (Contoh: penggunaan Security Information and Event Management) Jika KKM menggunakan platform berasaskan awan untuk mana-mana bahagian operasi, pengurusan log perlu menjadi tanggungjawab bersama antara penyedia perkhidmatan dan KKM.	Pentadbir Sistem ICT CSIRT IPKKM CSIRT Fasiliti KKM
8.16 AKTIVITI PEMANTAUAN *(MONITORING ACTIVITIES)*	**PERANAN**
8.16.1 Aktiviti Pemantauan Rangkaian, sistem dan aplikasi harus dipantau dan tindakan sewajarnya diambil untuk menilai kemungkinan insiden keselamatan maklumat telah berlaku. Pentadbir Sistem perlu memantau untuk mengesan tingkah laku tidak normal (anomali) dan kemungkinan berlaku insiden keselamatan maklumat. Aktiviti pemantauan perlu merangkumi perkara seperti yang berikut:	Pentadbir Sistem ICT Pentadbir Rangkaian Pentadbir Server CSIRT IPKKM CSIRT Fasiliti KKM

8.16 AKTIVITI PEMANTAUAN *(MONITORING ACTIVITIES)*	PERANAN
(a) trafik keluar *(outbound)* dan masuk *(inbound)* bagi rangkaian, sistem dan aplikasi; (b) capaian kepada sistem pelayan peralatan rangkaian, sistem pemantauan aplikasi kritikal (c) log daripada peralatan keselamatan (contohnya antivirus, IDS, sistem pencegahan pencerobohan (IPS), penapis web, firewall, pencegahan kebocoran data); (d) log peristiwa yang berkaitan dengan sistem dan aktiviti rangkaian; (e) memastikan kod sumber yang dilaksanakan telah diberi kebenaran untuk dilaksanakan dan tidak diubah tanpa kebenaran; dan (f) penggunaan dan prestasi sumber.	
8.16.2 Panduan mengenai Alat Pemantauan KKM perlu melaksanakan pemantauan dengan menggunakan alat pemantauan khas yang sesuai dengan jenis rangkaian dan trafik yang dikendalikannya. Alat pemantauan perlu dapat melaksanakan fungsi berikut: (a) berupaya untuk mengendalikan sejumlah besar data pemantauan; (b) berupaya bertindak balas terhadap data yang mencurigakan, corak penggunaan dan gelagat pengguna; (c) berupaya menghantar notifikasi tentang aktiviti tidak normal dalam persekitaran produksi melalui makluman proaktif dengan jumlah minimum palsu-positif (false-positive); dan (d) berupaya mengekalkan operasi pemantauan berterusan.	Pentadbir Sistem ICT Pentadbir Rangkaian Pentadbir Server CSIRT IPKKM CSIRT Fasiliti KKM
8.17 PENYELARASAN WAKTU *(CLOCK SYNCHRONIZATION)*	**PERANAN**
8.17.1 Penyelarasan Waktu Waktu bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut waktu piawai Malaysia. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam KKM atau domain keselamatan perlu diseragamkan dengan waktu piawai Malaysia yang ditetapkan oleh National Metrology Institute of Malaysia (NMIM).	Pentadbir Sistem ICT
8.18 PENGGUNAAN PROGRAM UTILITI ISTIMEWA *(USE OF PRIVILEGED UTILITY PROGRAMS)*	**PERANAN**
8.18.1 Penggunaan Program Utiliti yang Mempunyai Hak Istimewa Penggunaan program utiliti yang boleh mengatasi *(overriding)* kawalan sistem dan aplikasi hendaklah dikawal dan dipantau. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) penggunaan program utiliti perlu dihadkan kepada pengguna yang dipercayai dan dibenarkan;	Pengurus ICT Penyelaras ICT Fasiliti

8.18 PENGGUNAAN PROGRAM UTILITI ISTIMEWA *(USE OF PRIVILEGED UTILITY PROGRAMS)*	PERANAN
8.18.1 Penggunaan Program Utiliti yang Mempunyai Hak Istimewa Penggunaan program utiliti yang boleh mengatasi *(overriding)* kawalan sistem dan aplikasi hendaklah dikawal dan dipantau. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) penggunaan program utiliti perlu dihadkan kepada pengguna yang dipercayai dan dibenarkan; (b) penggunaan prosedur pengenalan, pengesahan dan kebenaran untuk program utiliti, termasuk pengenalan unik pengguna program utiliti; (c) mentakrif dan mendokumentasikan tahap kebenaran untuk program utiliti; (d) kebenaran untuk menggunakan program utiliti secara ad hoc; (e) melaksanakan pengasingan tugas dengan menghadkan capaian pengguna yang mempunyai capaian kepada program utiliti; (f) mengalih keluar atau melumpuhkan semua program utiliti yang tidak diperlukan; (g) menghadkan ketersediaan program utiliti; dan (h) memastikan semua aktiviti penggunaan program utiliti di log.	Pengurus ICT Penyelaras ICT Fasiliti
8.19 PEMASANGAN PERISIAN PADA SISTEM OPERASI *(INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS)*	**PERANAN**
8.19.1 Pemasangan Perisian pada Sistem yang Beroperasi Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus ialah seperti yang berikut: (a) strategi rollback perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian; (b) aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; (c) setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur; (d) pengemaskinian perisian operasi hanya boleh dilaksanakan oleh pentadbir terlatih atas kebenaran pengurusan; (e) memastikan bahawa hanya kod boleh laksana *(executable code)* yang telah diluluskan dan tiada kod pembangunan atau pengkompil (compiler) dipasang pada sistem operasi; (f) mengemas kini semua perpustakaan sumber *(source libraries)* program yang sepadan; (g) menggunakan sistem kawalan konfigurasi untuk mengekalkan kawalan semua perisian operasi serta dokumentasi sistem; dan	Pentadbir Sistem ICT Pegawai Aset Pegawai KKM

8.19 PEMASANGAN PERISIAN PADA SISTEM OPERASI *(INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS)*	PERANAN
(h) mengarkibkan versi lama perisian, bersama-sama dengan semua maklumat dan parameter, prosedur, butiran konfigurasi dan perisian sokongan yang diperlukan sebagai langkah luar jangka (contingency), dan selagi perisian itu diperlukan untuk membaca atau memproses data yang diarkibkan.	
8.19.2 Panduan mengenai Perisian Pihak ketiga Perkara berkaitan dengan perisian yang dibekalkan oleh pihak ketiga (Contoh: perisian yang digunakan untuk menjalankan mesin atau untuk tujuan perkhidmatan yang unik), semakan dan pematuhan terhadap garis panduan yang dibekalkan oleh pihak ketiga diperlukan bagi memastikan perisian kekal dalam keadaan terbaik. Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan pegawai, pembekal serta pihak yang mempunyai urusan dengan perkhidmatan ICT di KKM; (b) pihak ketiga yang memerlukan capaian kepada rangkaian KKM untuk memasang atau mengemas kini sesuatu perkara, aktiviti perlu dipantau dan dibenarkan mengikut kawalan; dan (c) perisian yang perlu dinaik taraf, dipasang atau ditampal perlu selari dengan prosedur KKM untuk menjamin konsistensi dengan seluruh perkhidmatan. (d) memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undangundang bertulis yang berkuatkuasa; dan (e) mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya. KKM perlu menggunakan versi perisian sumber terbuka yang terkini dan diselenggara secara aktif, jika perlu. KKM juga perlu mengambil kira sebarang risiko yang berkaitan dengan penggunaan perisian yang tidak diselenggara dalam operasi.	Pentadbir Sistem ICT Pegawai Aset Pengguna
8.20 KESELAMATAN RANGKAIAN *(NETWORK SECURITY)*	**PERANAN**
8.20.1 Keselamatan Rangkaian Rangkaian dan peranti rangkaian perlu dijamin, dikelola, dan dikawal untuk melindungi maklumat dalam sistem dan aplikasi. Perkara yang perlu dipatuhi adalah seperti berikut: (a) bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; (b) peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas daripada risiko seperti banjir, gegaran dan habuk;	

8.20 KESELAMATAN RANGKAIAN *(NETWORK SECURITY)*	PERANAN
(c) capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja; (d) semua peralatan rangkaian hendaklah melalui proses badan pengiktirafan yang berkaitan; (e) tembok keselamatan *(firewall)* hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian; (f) semua trafik keluar dan masuk rangkaian hendaklah melalui tembok keselamatan di bawah kawalan KKM; (g) semua perisian untuk menganalisis atau menawan paket rangkaian dilarang dipasang pada komputer pengguna KECUALI mendapat kebenaran; (h) memasang perisian IPS bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat Kerajaan; (i) memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; (j) sebarang penyambungan rangkaian yang bukan di bawah kawalan KKM tidak dibenarkan; (k) semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di KKM sahaja dan penggunaan modem (bagi sumber internet dari luar selain disediakan KKM) adalah dilarang sama sekali; (l) semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan; (m) menempatkan atau memasang antara muka *(interfaces)* yang bersesuaian antara rangkaian jabatan, rangkaian jabatan lain dan rangkaian awam; (n) mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; (o) kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja; (p) mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh; (q) mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan KKM; (r) mewujud dan melaksana kawalan pengalihan laluan *(routing control)* bagi memastikan pematuhan terhadap peraturan KKM. Semua peralatan yang hendak disambung kepada rangkaian perlu bebas daripada virus dan mempunyai antivirus yang sah; (s) capaian kepada rangkaian perlu dilaksanakan mengikutkategori yang telah ditetapkan iaitu Intranet, Internet dan Demilitarized Zone (DMZ); (t) sistem yang terdapat dalam rangkaian Intranet tidak dibenarkan dicapai dari Internet kecuali mendapat kebenaran dan kelulusan Ketua Jabatan serta mematuhi kawalan keselamatan semasa ;	Pentadbir Rangkaian

8.20 KESELAMATAN RANGKAIAN *(NETWORK SECURITY)*	PERANAN
(u) pihak ketiga tidak dibenarkan untuk mencapai rangkaian Intranet kecuali untuk kerja-kerja pembangunan atau penyelenggaraan sistem dengan kebenaran; dan (v) kemudahan capaian kepada rangkaian tanpa wayar hendaklah dipantau dan dikawal mengikut kategori penggunaannya.	
8.21 KESELAMATAN PERKHIDMATAN RANGKAIAN *(SECURITY OF NETWORK SERVICES)*	**PERANAN**
8.21.1 Keselamatan Perkhidmatan Rangkaian Pengurusan bagi semua perkhidmatan rangkaian dalaman dan sumber luar yang merangkumi mekanisme keselamatan dan tahap serta keperluan perkhidmatan rangkaian hendaklah dikenal pasti dan dimasukkan dalam perjanjian perkhidmatan. Langkah keselamatan rangkaian hendaklah merangkumi perkara berikut: (a) keperluan pengesahan rangkaian yang menentukan siapa, dari mana, dan bila akses dibenarkan; (b) kakitangan hendaklah memperoleh kelulusan terlebih dahulu sebelum mengakses perkhidmatan rangkaian, termasuk memastikan analisis proses kerja selesai dan kelulusan rasmi diperoleh; (c) penggunaan protokol pengurusan rangkaian yang kukuh bagi melindungi perkhidmatan daripada penyalahgunaan dan akses tanpa kebenaran; (d) kawalan akses istimewa bagi kakitangan yang dibenarkan menggunakan perkhidmatan rangkaian, sama ada dari jauh atau di tapak; (e) prosedur rekod log yang merekodkan maklumat berkaitan akses perkhidmatan rangkaian, termasuk identiti pengguna, masa, lokasi, dan data peranti yang digunakan; dan (f) pemantauan berterusan ke atas penggunaan perkhidmatan rangkaian bagi memastikan fungsi dan keselamatan sentiasa terjamin.	Pentadbir Rangkaian
8.22 PENGASINGAN RANGKAIAN *(SEGREGATION OF NETWORKS)*	**PERANAN**
8.22.1 Pengasingan Rangkaian Kelompok perkhidmatan maklumat, pengguna, dan sistem maklumat hendaklah diasingkan dalam rangkaian. KKM perlu mencapai keseimbangan antara keperluan operasi dan kawalan keselamatan apabila melaksanakan peraturan pengasingan rangkaian. Bagi memastikan pengasingan rangkaian yang berkesan, aspek berikut hendaklah diambil kira: (a) pemisahan Rangkaian kepada Sub-Rangkaian i. rangkaian hendaklah dibahagikan kepada sub-domain berdasarkan sensitiviti dan kepentingan setiap domain; ii. contoh klasifikasi termasuk "domain awam", "domain desktop", "domain pelayan", atau "sistem berisiko tinggi"; dan	Pentadbir Rangkaian

8.22 PENGASINGAN RANGKAIAN *(SEGREGATION OF NETWORKS)*	PERANAN
iii. pemisahan perlu mengambil kira keperluan perkhidmatan KKM seperti sumber manusia, ICT, dankewangan. (b) Perimeter Keselamatan dan Kawalan Akses i. sempadan bagi setiap sub-domain rangkaian hendaklah digambarkan dengan jelas; ii. sekiranya terdapat akses antara dua domain yang berbeza, sambungan perlu dihadkan di perimeter rangkaian melalui pintu masuk (gateway) seperti *firewall* atau *router;* dan iii. keperluan keselamatan setiap domain hendaklah dinilai sebelum menyediakan akses melalui *gateway*, selaras dengan Polisi Kawalan Akses (rujuk Bab 5). (c) Faktor Penilaian Keselamatan Penilaian keperluan pengasingan rangkaian hendaklah mengambil kira perkara berikut: i. tahap pengelasan aset maklumat; ii. kepentingan dan keutamaan maklumat; dan iii. kos serta faktor praktikal dalam menentukan teknologi *gateway* yang sesuai digunakan.	
8.22.2 Rangkaian Tanpa Wayar KKM perlu mempertimbangkan perkara berikut apabila mewujudkan parameter keselamatan rangkaian tanpa wayar: (a) membuat penilaian liputan sebelum melaksanakan segmentasi rangkaian tanpa wayar; (b) untuk rangkaian yang kompleks iaitu infrastruktur yang melibatkan pelbagai sub-domain, perkhidmatan dan sambungan dalaman serta luaran yang saling berhubung, KKM boleh membuat capaian tanpa wayar sebagai sambungan luaran dan tidak membenarkan capaian kepada rangkaian dalaman sehingga diberi kebenaran masuk melalui *gateway;* (c) untuk melindungi rangkaian yang sensitif, KKM boleh menetapkan bahawa semua percubaan capaian tanpa wayar diklasifikasikan sebagai sambungan dari luar, dan akses ke rangkaian dalaman tidak akan dibenarkan sehingga diluluskan secara sah melalui gateway. (d) capaian rangkaian tanpa wayar yang diberikan kepada pegawai dan pelawat hendaklah diasingkan; dan (e) pelawat hendaklah tertakluk kepada peraturan KKM mengenai perkhidmatan *Wi-Fi.*	Pentadbir Rangkaian
8.23 PENAPISAN WEB *(WEB FILTERING)*	**PERANAN**
8.23.1 Penapisan Web Kawalan penapisan web dalam bentuk perisian atau sebagainya perlu dilaksanakan bagi mengesan dan menyekat capaian ke kategori laman web yang boleh mengganggu produktiviti kerja, menggunakan *bandwidth*	

8.23 PENAPISAN WEB *(WEB FILTERING)*	PERANAN
secara berlebihan, atau melanggar dasar etika dan profesionalisme KKM. Contoh laman web adalah seperti berikut: (a) Laman Web Hiburan Melampau: Laman web video, permainan dalam talian yang tidak berkaitan dengan kerja; (b) Laman Web Dewasa/Lucah: Laman web dengan kandungan eksplisit; dan (c) Laman web tidak selamat: Laman web dengan ancaman *(phishing, virus)*. Perkara ini dilakukan bagi melindungi sistem maklumat daripada sebarang ancaman keselamatan dan memastikan penggunaan sumber rangkaian yang bertanggungjawab dan produktif oleh pegawai. KKM hendaklah mengenal pasti jenis laman web yang patut atau tidak boleh dicapai oleh pegawai. KKM hendaklah mempertimbangkan untuk menyekat capaian kepada jenis laman web yang berikut : (a) laman web yang mempunyai fungsi muat naik maklumat melainkan dibenarkan atas sebab perkhidmatan yang sah; (b) tapak web yang diketahui atau disyaki berniat jahat; (c) pelayan arahan dan kawalan (command and control); (d) laman web berniat jahat yang diperoleh daripada risikan ancaman; dan (e) laman web yang berkongsi kandungan haram.	Pentadbir Rangkaian Pentadbir Keselamatan
8.24 PENGGUNAAN KRIPTOGRAFI *(USE OF CRYPTOGRAPHY)*	**PERANAN**
8.24.1 Penggunaan Kriptografi Kawalan ini perlu dalam memastikan kerahsiaan, integriti, ketulenan dan ketersediaan aset maklumat adalah terpelihara. melalui penggunaan aplikasi kriptografi yang betul dan tepat. Perkara yang perlu dipertimbangkan oleh KKM apabila menggunakan kaedah kriptografi: (a) perlu merujuk kepada dasar, arahan, serta garis panduan semasa yang sedang berkuatkuasa mengenai penggunaan kriptografi untuk memaksimumkan faedahnya dan mengurangkan risiko.; (b) mesti mengambil kira kompleksiti sumber maklumat serta tahap pengelasan maklumat yang ditetapkan (contohnya, Rahsia Besar, Rahsia, Sulit, Terhad) apabila memilih jenis, kekuatan dan kualiti algoritma penyulitan; (c) menggunakan pendekatan kriptografi secara mandatori apabila memindahkan maklumat ke peranti mudah alih, peralatan media, atau apabila ia disimpan di dalamnya; (d) perlu menangani sebarang perkara yang berkaitan dengan pengurusan kekunci, seperti membentuk dan melindungi kunci kriptografi, termasuk proses pembentukan, perlindungan (penyimpanan selamat, pengedaran, pelupusan), dan mempunyai skema pemulihan data yang terancang sekiranya kunci itu hilang atau terdedah;	Pemilik Sistem Pentadbir Sistem ICT


“Anda tidak boleh melindungi sesuatu yang anda tidak fahami.”
- Ross Anderson


“Kesedaran siber ialah
antivirus yang terbaik.”
- Mikka Hypponen

8.24 PENGGUNAAN KRIPTOGRAFI *(USE OF CRYPTOGRAPHY)*	PERANAN
(e) hendaklah menentukan peranan dan tanggungjawab yang jelas untuk perkara berikut: (i) peraturan untuk menggunakan teknik kriptografi mesti diwujudkan, didokumentasikan dan dikuatkuasakan secara konsisten.; dan (ii) proses pengendalian kunci, termasuk penjanaan, penyimpanan, penggunaan, pengedaran, dan pemansuhan kekunci. (f) mengguna pakai dan membenarkan piawaian merangkumi algoritma kriptografi, kekuatan sifer (cipher) dan amalan penggunaan kriptografi.	
8.24.2 Kaedah Kriptografi Kriptografi merangkumi kaedah-kaedah seperti yang berikut: (a) penyulitan Data: Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat penyulitan semasa dalam simpanan atau semasa sedang dipindahkan; dan (b) tandatangan Digital digunakan bagi memastikan ketulenan dan integrity maklumat digital serta memberikan bukti tidak boleh disangkal. Ini membolehkan pengesahan bahawa maklumat tersebut berasal dari sumber yang sah dan tidak diubah suai	Pemilik Sistem Pentadbir Sistem ICT
8.24.3 Pengurusan Infrastruktur Kunci Awam Pengurusan ke atas Pengurusan Infrastruktur Kunci Awam (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah sijil digital tersebut.	Pemilik Sistem Pentadbir Sistem ICT
8.24.4 Kelebihan dalam Kriptografi Kriptografi boleh digunakan untuk membantu KKM mencapai empat (4) objektif keselamatan maklumat. Objektif ini termasuk mengesahkan ketulenan kunci awam melalui proses pengurusan kunci awam: (a) kriptografi memastikan kerahsiaan data terpelihara sama ada semasa dalam transit *(data in transit)* atau apabila disimpan *(data at rest)*, menghalang capaian atau pendedahan tanpa kebenaran. (b) penggunaan tandatangan digital menjamin bahawa maklumat yang disampaikan adalah tulen, tidak diubah suai, dan boleh dipercayai sepanjang kitaran hayatnya. (c) kaedah kriptografi menyediakan jaminan kukuh bahawa semua peristiwa atau tindakan yang diambil, termasuk penghantaran dan penerimaan maklumat, tidak boleh disangkal oleh pihak yang terlibat (d) pengesahan melalui kaedah kriptografi membolehkan KKM mengesahkan identiti pengguna secara sah sebelum mereka diberikan capaian kepada sistem dan aplikasi, seterusnya melindungi daripada capaian tanpa kebenaran	Pemilik Sistem Pentadbir Sistem ICT

8.25 KITARAN HAYAT PEMBANGUNAN SELAMAT *(SECURE DEVELOPMENT LIFE CYCLE)*	PERANAN
8.25.1 Kitaran Hayat Pembangunan Selamat Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan bagi memastikan kitar hayatpembangunan yang selamat. Perkara yang perlu dipertimbangkan oleh KKM adalah seperti yang berikut: (a) persekitaran pembangunan, pengujian dan produksi hendaklah diasingkan; (b) jabatan perlu memberikan panduan berkaitan: (i) keselamatan adalah faktor penting dalam pembangunan sistem. Oleh itu, ia mesti diambil kira dalam kitar hayat pembangunan sistem ; (ii) memastikan setiap bahasa pengaturcaraan mempunyai pengekodan selamat yang mematuhi kawalan. (c) melaksanakan keperluan keselamatan berdasarkan Bab 5 semasa fasa spesifikasi dan reka bentuk; (d) menyediakan senarai semak keselamatan berdasarkan Bab 5; (e) terlibat dalam pengujian keselamatan dan sistem, seperti pengujian penembusan dan pengimbasan kod sumber sejajar dengan Kawalan; (f) perlu mewujudkan repositori selamat untuk menyimpan kod sumber dan konfigurasi mengikut Kawalan; (g) perlu memastikan keselamatan dalam kawalan versi; (h) perlu menjamin semua pegawai yang terlibat dalam pembangunan sistem mempunyai pengetahuan yang diperlukan mengenai keselamatan aplikasi dan latihan yang bersesuaian seperti yang ditakrifkan dalam Bab 8; (i) memastikan pembangun sistem/aplikasi perlu mempunyai keupayaan untuk mengenali dan mengelakkan kelemahan keselamatan dalam pembangunan sistem menurut Bab 8; dan (j) perlu mematuhi peraturan pelesenan, dan menilai sama ada terdapat sebarang alternatif yang berdaya maju dan menjimatkan kos, menurut Bab 8. Jika KKM memutuskan untuk melaksanakan pembangunan sistem secara penyumberan luar, pembekal yang dilantik perlu mematuhi peraturan dan prosedur dalam pembangunan aplikasi dan sistem yang selamat.	Pentadbir Sistem ICT Pembangun Sistem
8.26 KEPERLUAN KESELAMATAN APLIKASI *(APPLICATION SECURITY REQUIREMENTS)*	**PERANAN**
8.26.1 Keperluan Keselamatan Aplikasi Keperluan keselamatan maklumat perlu dikenal pasti, dinyatakan, dan diluluskan semasa membangunkan atau semasa melaksanakan perolehan aplikasi. KKM perlu menjalankan penilaian risiko untuk menetapkan keperluan keselamatan maklumat yang diperlukan untuk aplikasi. Pelaksanaan penilaian risiko perlulah mengikut arahan, peraturan, dasar dan undang undang berkaitan yang sedang berkuatkuasa.	Pentadbir Sistem ICT

8.26 KEPERLUAN KESELAMATAN APLIKASI *(APPLICATION SECURITY REQUIREMENTS)*	PERANAN
8.26.1 Keperluan Keselamatan Aplikasi Keperluan keselamatan maklumat perlu dikenal pasti, dinyatakan, dan diluluskan semasa membangunkan atau semasa melaksanakan perolehan aplikasi. KKM perlu menjalankan penilaian risiko untuk menetapkan keperluan keselamatan maklumat yang diperlukan untuk aplikasi. Pelaksanaan penilaian risiko perlulah mengikut arahan, peraturan, dasar dan undang undang berkaitan yang sedang berkuatkuasa. Perkara yang perlu dipertimbangkan dalam melindungi keselamatan maklumat aplikasi adalah seperti berikut: (a) merujuk kepada Bab 5 dan 8, dalam memperuntukkan capaian kepada identiti entiti tertentu; (b) pengelasan aset maklumat yang akan disimpan atau dikendalikan oleh aplikasi mesti dikenal pasti; (c) keperluan untuk memisahkan capaian kepada ciri dan data yang disimpan dalam aplikasi; (d) menilai pertahanan aplikasi terhadap penembusan siber seperti suntikan SQL atau pemintasan yang tidak diingini seperti limpahan penimbal *(buffer overflow)*; (e) perlu memenuhi segala arahan, garis panduan, piawaian kawal selia dan undang-undang apabila melibatkan transaksi yang diproses, dijana, disimpan atau dikeluarkan oleh aplikasi; (f) memastikan data sulit dilindungi; (g) memastikan keselamatan maklumat apabila ia digunakan, dipindahkan atau disimpan; (h) semua pihak yang berkaitan perlu melaksanakan kaedah penyulitan yang selamat ; (i) melaksanakan kawalan input, seperti mengesahkan input dan melaksanakan pemeriksaan integriti bagi menjamin ketepatan; (j) memastikan hak capaian, serta siapa yang boleh melihat output, diambil kira untuk kawalan output; (k) adalah penting untuk mengenakan had ke atas perkara yang boleh dimasukkan dalam medan "teks bebas" untuk melindungi daripada pengedaran maklumat sulit yang tidak disengajakan; (l) keperluan kawal selia, seperti kawalan log transaksi dan bukan-sangkalan (non-repudiation); (m) kawalan keselamatan lain mungkin memerlukan pematuhan kepada keperluan khusus; contohnya, sistem pengesanan kebocoran data; dan (n) melaksana kaedah yang bersesuaian dalammengendalikan mesej ralat.	Pentadbir Sistem ICT
8.26.2 Perkhidmatan berkaitan Transaksi Perkara yang perlu dipertimbangkan sekiranya menyediakan perkhidmatan yang melibatkan transaksi adalah seperti berikut:	

8.26 KEPERLUAN KESELAMATAN APLIKASI *(APPLICATION SECURITY REQUIREMENTS)*	PERANAN
(a) tahap kepercayaan yang perlu ada pada setiap pihak terhadap identiti pihak lain adalah penting dalam sebarang transaksi; (b) kebolehpercayaan data yang dihantar atau diproses mesti terjamin dan mekanisme atau teknologi yang sesuai untuk mengesan dan mencegah defisit integriti mestilah digunakan seperti pencincangan *(hashing)* dan tandatangan digital; (c) menentukan pegawai yang diberi kuasa untuk meluluskan, menandatangani dan mengesahkan dokumen transaksi kritikal; (d) memastikan kerahsiaan dan ketepatan dokumen penting serta mengesahkan penghantaran dan penerimaan dokumen tersebut; (e) memelihara kerahsiaan dan ketepatan transaksi seperti contoh pesanan dan invois; (f) transaksi mesti kekal sulit untuk tempoh masa tertentu; dan (g) obligasi kontrak mesti dipenuhi.	Pentadbir Sistem ICT
8.26.3 Pemesanan Elektronik dan Aplikasi Pembayaran KKM perlu mempertimbangkan perkara berikut apabila memasukkan keupayaan pembayaran dan pesanan elektronik ke dalam aplikasi: (a) memastikan kerahsiaan dan integriti maklumat pesanan; (b) mewujudkan tahap pengesahan yang sesuai untuk mengesahkan maklumat pembayaran yang diberikan oleh pelanggan; (c) mengelakkan salah letak atau replikasi data transaksi; (d) memastikan maklumat dilindungi daripada pendedahan tidak sengaja atau akses yang tidak sah disebabkan diletakkan di ruangan umum; dan (e) sekiranya menggunakan perkhidmatan luar untuk mengeluarkan tandatangan digital, ciri-ciri keselamatan perlu di integrasikan di sepanjang proses tersebut	Pentadbir Sistem ICT
8.27 PRINSIP SENI BINA DAN KEJURUTERAAN SISTEM YANG SELAMAT *(SECURE SYSTEM ARCHITECTURE AND ENGINEERING PRINCIPLES)*	**PERANAN**
8.27.1 Prinsip Seni bina dan Kejuruteraan Sistem yang Selamat Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada Garis Panduan dan Pelaksanaan Independent Verification and Validation (IV&V) sektor awam yang terkini.Kawalan ini juga turut terpakai kepada sistem yang dibangunkan oleh pihak ketiga. Kawalan ini memerlukan prinsip kejuruteraan sistem yang selamat merangkumi perkara seperti berikut: (a) kaedah pengesahan pengguna;	Pemilik Sistem Pembangun Sistem Pentadbir Sistem ICT

8.27 PRINSIP SENI BINA DAN KEJURUTERAAN SISTEM YANG SELAMAT *(SECURE SYSTEM ARCHITECTURE AND ENGINEERING PRINCIPLES)*	PERANAN
(b) panduan kawalan sesi selamat; (c) prosedur untuk sanitasi dan mengesahkan data; (d) analisis menyeluruh terhadap kawalan keselamatan yang direka untuk melindungi sistem daripada kerentanan dan ancaman yang dikenalpasti; (e) penilaian terhadap keberkesanan kawalan keselamatan dalam mencegah, mengesan dan bertindak balas terhadap insiden keselamatan.; (f) melaksanakan tinjauan keselamatan terhadap keperluan proses perkhidmatan dalam mengadaptasi teknologi khusus seperti penyulitan maklumat; (g) mengenal pasti bagaimana kawalan keselamatan akan dilaksanakan; dan (h) mengenal pasti bagaimana kawalan keselamatan dapat beroperasi dalam membentuk sistem pertahanan yang komprehensif.	
8.27.2 Prinsip *Zero Trust* Penggunaan prinsip ini adalah seperti berikut: (a) pendekatan keselamatan perlu dibina berdasarkan andaian bahawa sistem KKM terjejas dan keselamatan perimeter rangkaian yang ditetapkan tidak dapat memberikan perlindungan yang mencukupi; (b) polisi "pengesahan sebelum kepercayaan" perlu diguna pakai apabila memberikan capaian kepada sistem maklumat. Ini bertujuan memastikan bahawa capaian hanya diberikan selepas proses pengesahan yang rapi, bagi memastikan hanya pengguna yang sah dan dibenarkan mempunyai capaian.; (c) memberikan jaminan bahawa capaian kepada sistem maklumat dilindungi dengan penyulitan hujung ke hujung; (d) mekanisme pengesahan dilaksanakan dengan mengandaikan capaian adalah dari luar atau rangkaian terbuka; (e) prinsip had capaian minimum *(least privilege)* dan kawalan capaian dinamik hendaklah dilaksanakan secara konsisten selaras dengan Bab 5 (Kawalan Capaian dan Hak Capaian) dan Bab 8 (Hak Capaian Istimewa). Pelaksanaan ini perlu merangkumi proses pengesahan dan kebenaran ke atas sistem maklumat dan maklumat sensitif, dengan mengambil kira konteks seperti identiti pengguna dan pengelasan maklumat; dan (f) identiti pihak yang membuat permintaan capaian hendaklah disahkan, dan permintaan kebenaran akses kepada sistem maklumat perlu disemak berdasarkan maklumat pengesahan, selaras dengan Bab 5 (Pengesahan Maklumat dan Pengurusan Identiti) dan Bab 8 (Pengesahan Selamat).	Pemilik Sistem Pembangun Sistem Pentadbir Sistem ICT
8.27.3 Teknik Kejuruteraan Sistem Selamat KKM perlu mempertimbangkan perkara berikut:	Pemilik Sistem Pembangun Sistem Pentadbir Sistem ICT

8.27 PRINSIP SENI BINA DAN KEJURUTERAAN SISTEM YANG SELAMAT *(SECURE SYSTEM ARCHITECTURE AND ENGINEERING PRINCIPLES)*	PERANAN
(a) penting untuk menggabungkan prinsip seni bina selamat seperti "keselamatan melalui reka bentuk *(security by design)*", "pertahanan secara mendalam *(defence in depth)*", "gagal dengan selamat *(fail securely)*", "input tidak percaya daripada aplikasi luaran *(distrust input from external applications)*", "anggap pelanggaran *(assume breach)*", "hak keistimewaan paling rendah *(least privilege)*", "kebolehgunaan dan kebolehurusan *(usability and manageability)*" dan "fungsi paling sedikit *(least functionality)*"; (b) menjalankan semakan reka bentuk berorientasikan keselamatan untuk mengesan sebarang isu keselamatan maklumat dan memastikan langkah keselamatan diwujudkan dan memenuhi keperluan keselamatan; (c) mendokumentasikan dan mengakui langkah keselamatan yang gagal memenuhi keperluan; dan (d) pengukuhan sistem adalah penting untuk keselamatan mana-mana sistem.	

8.28 PENGEKODAN SELAMAT *(SECURE CODING)*	PERANAN
8.28.1 Pengekodan Selamat KKM perlu melaksanakan proses pengekodan selamat ke atas perisian atau sistem yang dibangunkan secara dalaman *(inhouse)* atau penyumberan luar *(outsource)* bagi melindungi aset dan maklumat. KKM perlu mempertimbangkan prasyarat pengekodan selamat seperti berikut: (a) prinsip pengekodan selamat perlu disesuaikan ke atas pembangunan sistem/aplikasi secara dalaman dan secara penyumberan luar *(outsourcing)*; (b) mengenal pasti dan mendokumenkan kesilapan reka bentuk pengekodan yang paling umum *(default)*, lama *(old programming)* serta amalan pengekodan yang lemah untuk mengelakkan pelanggaran keselamatan data; (c) melaksanakan dan mengkonfigurasi alat pembangunan perisian seperti Persekitaran Pembangunan Bersepadu *(Integrated Development Environment-IDE)* bagi memastikan keselamatan semua kod yang dicipta; (d) menggunakan kod perpustakaan *(code library)* yang diluluskan dan disahkan sahaja (e) alat pembangunan perisian perlu menyediakan panduan dan arahan untuk membantu KKM dalam mematuhi garis panduan dan arahan; dan (f) alat pembangunan seperti penyusun *(compiler)* hendaklah disemak, diselenggara dan digunakan dengan selamat oleh KKM.	Pentadbir Sistem ICT Pemilik Sistem

8.28 PENGEKODAN SELAMAT *(SECURE CODING)*	PERANAN
8.28.2 Amalan Pengekodan Selamat Perkara berikut perlu dipertimbangkan dalam memastikan amalan dan prosedur pengekodan selamat semasa proses pengekodan: (a) prinsip pengekodan selamat untuk perisian selamat perlu disesuaikan dengan bahasa pengaturcaraan dan teknik pengaturcaraan; (b) melaksanakan teknik pengaturcaraan berstruktur; (c) dilarang menggunakan kaedah pengekodan sistem yang tidak selamat seperti sampel kod yang tidak diluluskan atau kata laluan secara *hard-coded;* dan (d) ujian keselamatan hendaklah dijalankan semasa pembangunan dan pengujian penerimaan sistem seperti yang dinyatakan dalam Bab 8. KKM perlu mengenal pasti perkara seperti berikut sebelummelancarkan sistem dalam persekitaran produksi *(production)*: (a) adakah terdapat kerentanan yang mendedahkan sistem kepada serangan permukaan *(attack surface)*?; (b) adakah prinsip hak capaian yang paling minimum dipatuhi?; dan (c) mengenal pasti dan mendokumenkan ralat dan kerentanan reka bentuk pengekodan serta amalan pengekodan yang tidak selamat untuk mengelakkan pelanggaran keselamatan data.	Pentadbir Sistem ICT Pemilik Sistem
8.28.3 Semakan Pengekodan Selamat Pelaksanaan Pengekodan dalam Persekitaran Produksi *(production)*: (a) kemas kini sistem *(system update)* dan perisian hendaklah dilaksanakan menggunakan kaedah yang selamat dan terkawal, termasuk pengesahan sumber kemas kini, pengujian sebelum pelaksanaan, dan pemantauan selepas kemas kini dilakukan; (b) sebarang kelemahan dan kerentanan keselamatan yang dikenal pasti dalam sistem, aplikasi, atau komponen ICT hendaklah ditangani dengan segera berdasarkan keutamaan risiko, sejajar dengan Bab 8; (c) KKM hendaklah menyimpan dan menyelenggara rekod lengkap berkenaan insiden, potensi serangan, percubaan capaian tidak sah dan ralat sistem kritikal. Rekod ini perlu disemak secara berkala bagi membolehkan tindakan pembetulan, pengemaskinian kawalan, atau pelarasan sistem dilaksanakan; dan (d) penggunaan alatan keselamatan *(security tools)* seperti kawalan capaian, pengurusan log, dan sistem pengurusan versi hendaklah dikuatkuasakan bagi menghalang sebarang capaian, penggunaan atau pengubahsuaian kod sumber tanpa kebenaran.	Pentadbir Sistem ICT Pemilik Sistem
8.29 UJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN *(SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE)*	**PERANAN**
8.29.1 Pengujian Keselamatan Sistem KKM perlu melaksanakan ujian keselamatan semasa proses pembangunan dan pengujian penerimaan sistem bagi menjamin bahawa sistem maklumat	

8.29 UJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN *(SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE)*	PERANAN
yang baharu, versi baharu/kemas kini, memenuhi keperluan keselamatan maklumat apabila ia berada dalam persekitaran produksi *(production)*. Sebagai sebahagian daripada kawalan keselamatan dalam pembangunan dan penyelenggaraan sistem, ujian keselamatan hendaklah merangkumi tiga (3) komponen utama berikut: (a) Kawalan Akses dan Perlindungan Data i. Melaksanakan pengesahan pengguna yang kukuh dan bersesuaian, seperti yang digariskan dalam Bab 8; ii. Mempunyai mekanisme sekatan capaian berdasarkan keperluan peranan dan fungsi, selaras dengan Bab 8; dan iii. Melaksanakan langkah perlindungan data melalui kriptografi, menurut keperluan Kawalan Penggunaan Kriptografi. (b) Pengaturcaraan Selamat Sistem dan aplikasi yang dibangunkan hendaklah diuji bagi memastikan kod ditulis secara selamat, bebas daripada kerentanan yang boleh dieksploitasi (contohnya SQL injection, XSS, buffer overflow), dan mematuhi prinsip-prinsip pengaturcaraan selamat seperti yang ditetapkan dalam Bab 8. (c) Konfigurasi Sistem dan Infrastruktur yang Selamat i. Bab 8 – Pengurusan Konfigurasi ii. Bab 8 – Keselamatan Rangkaian iii. Bab 8 – Pengasingan Rangkaian Konfigurasi ini termasuk tetapi tidak terhad kepada penggunaan *firewall*, pengurusan *port* dan servis, serta penetapan konfigurasi persekitaran rangkaian yang selamat.	Pemilik Sistem Pentadbir Sistem ICT Pembangun Sistem
8.29.2 Pembangunan Secara Penyumberluaran *(Outsourcing)* KKM perlu mematuhi prosedur perolehan yang ketat apabila mendapatkan khidmat dari pihak ketiga atau perolehan komponen ICT *(hardware & software)* dari sumber luar KKM. KKM perlu memastikan pihak ketiga mempersetujui perjanjian perkhidmatan yang disediakan dan memenuhi kriteria kawalan keselamatan maklumat seperti yang ditetapkan dalam Bab 5. KKM perlu menjamin bahawa perkhidmatan dan komponen ICT yang dibekalkan oleh pihak ketiga adalah selaras dengan piawaian keselamatan bagi keselamatan maklumat.	Pemilik Sistem Pentadbir Sistem ICT Pembangun Sistem
8.29.3 Pembangunan Secara Dalaman *(In-House)* Pasukan pembangun dalaman perlu menjalankan ujian keselamatan awal untuk menjamin keselamatan dalam sistem ICT yang dibangunkan secara dalaman dan mematuhi spesifikasi keselamatan. Pusingan pertama ujian perlu dijalankan, diikuti dengan ujian penerimaan bebas selaras dengan Bab 5. Dalam konteks pembangunan dalaman, pasukan perlu mengambil kira langkah-langkah berikut:	Pemilik Sistem Pentadbir Sistem ICT Pembangun Sistem

8.29 UJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN *(SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE)*	PERANAN
8.29.3 Pembangunan Secara Dalaman *(In-House)* Pasukan pembangun dalaman perlu menjalankan ujian keselamatan awal untuk menjamin keselamatan dalam sistem ICT yang dibangunkan secara dalaman dan mematuhi spesifikasi keselamatan. Pusingan pertama ujian perlu dijalankan, diikuti dengan ujian penerimaan bebas selaras dengan Bab 5. Dalam konteks pembangunan dalaman, pasukan perlu mengambil kira langkah-langkah berikut: (a) Semakan Kod *(Secure Code Review)* - Menjalankan semakan kod sumber secara sistematik bagi mengenal pasti dan menangani isu keselamatan, khususnya pada aspek berkaitan input pengguna, pengendalian ralat, serta aliran logik yang dijangkakan dan luar jangka (expected and edge-case scenarios). (b) Imbasan Kerentanan *(Vulnerability Scanning)* - Melaksanakan imbasan terhadap persekitaran pembangunan, tetapan konfigurasi, dan perisian yang digunakan untuk mengenal pasti kelemahan seperti berikut: i. Tetapan tidak selamat *(misconfigured services)* ii. Komponen usang atau tidak ditampal *(unpatched components)* (c) Ujian Penembusan *(Penetration Testing)* - Menjalankan ujian penembusan yang disasarkan untuk: i. Mengenal pasti kelemahan dalam logik aplikasi, kod, dan reka bentuk keselamatan ii. Mengesahkan sama ada kawalan keselamatan sedia ada boleh ditembusi iii. Menilai daya tahan sistem terhadap serangan sebenar	Pemilik Sistem Pentadbir Sistem ICT Pembangun Sistem
8.29.4 Panduan Sokongan KKM perlu mempertimbangkan penyediaan persekitaran ujian untuk menjalankan pelbagai jenis ujian, termasuk ujian fungsi, ujian bukan-fungsi dan ujian prestasi. Persekitaran ujian maya boleh diwujudkan dengan konfigurasi untuk menguji sistem ICT dalam senario persekitaran operasi yang berbeza dan melaksanakan penambahbaikan tetapan dengan sewajarnya.	Pemilik Sistem Pentadbir Sistem ICT Pembangun Sistem
8.30 PEMBANGUNAN SUMBER LUAR *(OUTSOURCED DEVELOPMENT)*	**PERANAN**
8.30.1 Pembangunan Sumber Luar KKM hendaklah sentiasa memantau dan mengesahkan bahawa kerja pembangunan secara penyumberan luar *(outsourcing)* memenuhi keperluan keselamatan maklumat yang ditetapkan oleh arahan, garis panduan, piawaian yang ditetapkan. Perkara yang perlu dipertimbangkan sekiranya menggunakan perkhidmatan pembangunan sumber luar: (a) perjanjian lesen, kod sumber ialah HAK MILIK KERAJAAN dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi;	Pengurus ICT Penyelaras ICT Fasiliti Pemilik Sistem

8.30 PEMBANGUNAN SUMBER LUAR *(OUTSOURCED DEVELOPMENT)*	PERANAN
(b) bagi semua perkhidmatan yang disediakan oleh sumber luar, termasuk *Software as a Service (SaaS)* yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah menetapkan keperluan mandatori supaya pembekal memberikan Kerajaan hak untuk mengakses kod sumber serta melaksanakan penilaian dan pengurusan risiko; (c) keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik; (d) menjalankan prosedur ujian penerimaan (*UAT*, *FAT*, dll) berdasarkan kepada kualiti dan ketepatan serahan sistem; (e) memastikan kod sumber perisian dilindungi dengan perjanjian escrow *(escrow agreement)*. Sebagai contoh, ia mungkin menangani perkara yang akan berlaku jika pihak ketiga berhenti beroperasi; (f) mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian; (g) menyediakan model ancaman *(threat modelling)* untuk dipertimbangkan oleh pembangun sistem serta memastikan tahap keselamatan minimum yang boleh diterima; (f) mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian; (g) menyediakan model ancaman *(threat modelling)* untuk dipertimbangkan oleh pembangun sistem serta memastikan tahap keselamatan minimum yang boleh diterima; (h) menyediakan bukti bahawa ujian yang mencukupi telah dilaksanakan ke atas perisian atau sistem ICT bagi mengawal kehadiran kandungan berniat jahat; (i) menyediakan bukti bahawa ujian yang mencukupi telah dilaksanakan ke atas perisian atau sistem ICT bagi menangani kerentanan yang dikenal pasti; (j) sebagai sebahagian daripada perjanjian dengan pihak ketiga, KKM perlu dibenarkan untuk mengaudit proses pembangunan dan kawalan; (k) keperluan keselamatan untuk persekitaran pembangunan harus diwujudkan dan dilaksanakan; dan (l) perlu mempertimbangkan undang-undang, dan peraturan yang berkenaan.	
8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PRODUKSI *(SEPARATION OF DEVELOPMENT, TEST AND PRODUCTION ENVIRONMENTS)*	**PERANAN**
8.31.1 Pengasingan Persekitaran Pembangunan, Pengujian dan Produksi Persekitaran pembangunan, pengujian dan produksi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau berlaku perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut:	

8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PRODUKSI *(SEPARATION OF DEVELOPMENT, TEST AND PRODUCTION ENVIRONMENTS)*	PERANAN
8.31.1 Pengasingan Persekitaran Pembangunan, Pengujian dan Produksi Persekitaran pembangunan, pengujian dan produksi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau berlaku perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) peraturan dan prosedur kebenaran mesti dirangka, didokumenkan dan dilaksanakan berkenaan penggunaan perisian dalam persekitaran produksi selepas ia melalui persekitaran pembangunan; (b) pengujian dalam persekitaran produksi tidak perlu dilaksanakan melainkan ia telah ditentukan dengan teliti dan mendapat kebenaran terlebih dahulu; (c) alat pembangunan seperti penyusun *(compiler)* dan penyunting *(editor)*, tidak boleh disediakan dalam persekitaran produksi melainkan ia benar-benar diperlukan; dan (d) untuk mengurangkan kesilapan, label persekitaran yang betul perlu dipaparkan dengan jelas dalam menu.	Pentadbir Sistem ICT
8.31.2 Persekitaran Pembangunan Selamat KKM perlu melindungi persekitaran pembangunan dan pengujian daripada potensi bahaya keselamatan dengan mengambil kira perkara berikut: (a) pastikan semua alat pembangunan, integrasi dan pengujian sentiasa ditampal *(patch)* dan dikemaskini; (b) pastikan semua sistem dan perisian disediakan dalam keadaan yang selamat; (c) kawalan yang sesuai mesti dilaksanakan untuk tujuan capaian kepada persekitaran; (d) perubahan kepada persekitaran dan kodnya perlu dipantau dan disemak; (e) pemantauan dan kajian semula persekitaran yang selamat perlu dilakukan; dan (f) persekitaran perlu dilindungi dengan sandaran. Tiada individu perlu diberi kelulusan prerogatif untuk membuat perubahan kepada kedua-dua persekitaran pembangunan dan produksi tanpa mendapat kelulusan terlebih dahulu. Untuk mengelakkan ini, KKM boleh memisahkan hak capaian atau meletakkan dan melaksanakan kawalan capaian. Kawalan teknikal selanjutnya adalah memastikan semua aktiviti capaian di log dan memantau capaian kepada persekitaran secara masa nyata.	Pentadbir Sistem ICT
8.31.3 Panduan Sokongan Kepada Pembangun dan Penguji Sistem Perkara yang perlu dipertimbangkan adalah:	

8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PRODUKSI *(SEPARATION OF DEVELOPMENT, TEST AND PRODUCTION ENVIRONMENTS)*	PERANAN
(a) perlu menetapkan peranan khusus dan menguatkuasakan pengasingan tugas antara pembangun dan penguji; (b) perlu membuat tetapan bagi menghalang pembangun sistem daripada mencapai persekitaran produksi yang menyimpan dan memproses data sebenar yang sensitif. Perkara ini diperlukan untuk mengawal perubahan yang tidak disengajakan pada fail atau tetapan sistem, menjalankan kod yang tidak dibenarkan yang boleh mendedahkan data sensitif; (c) pasukan pembangun dan penguji boleh berisiko menjejaskan data produksi yang sulit jika menggunakan peranti pengkomputeran yang sama;dan (d) keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem.	Pentadbir Sistem ICT

8.32 PENGURUSAN PERUBAHAN *(CHANGE MANAGEMENT)*	PERANAN
8.32.1 Pengurusan Perubahan Semua pengubahsuaian kepada sistem maklumat serta pelaksanaan sistem baharu, perlu mematuhi peraturan dan prosedur yang ditetapkan. Butiran perubahan ini mesti dinyatakan dan didokumenkan secara jelas. Selain itu, mesti melalui proses penilaian dan jaminan kualiti. Perkara yang perlu untuk dipertimbangkan oleh KKM dalam prosedur pengurusan perubahan adalah seperti berikut: (a) menilai potensi kesan pengubahsuaian yang dicadangkan dengan mengambil kira semua kebergantungan sistem tersebut; (b) melaksanakan kawalan kebenaran untuk perubahan. Pastikan semua pengubahsuaian dibenarkan oleh pegawai yang berkenaan. Pastikan hanya pegawai yang diberi kuasa mempunyai capaian kepada sistem dan semua perubahan didokumenkan dengan betul; (c) memaklumkan kepada pasukan dalam dan kumpulan luar tentang perubahan yang dicadangkan; (d) memastikan pematuhan kepada kawalan dengan membangun dan melaksanakan ujian dan ujian penerimaan untuk pengubahsuaian; (e) mewujudkan pelan dan prosedur kecemasan dan kontigensi, termasuk prosedur berbalik *(fall-back)*; (f) mengekalkan rekod semua perubahan dan aktiviti berkaitan; (g) memastikan pematuhan kepada Kawalan Dokumentasi Prosedur, mendokumentasi, menyemak peranan pengguna dan dipinda mengikut keperluan; dan (h) menilai dan mengemaskini pelan kesinambungan ICT dan prosedur pemulihan serta tindak balas agar selari dengan pengubahsuaian yang telah dilaksanakan.	Pemilik Aset Pemilik Sistem Pentadbir Sistem ICT

8.32 PENGURUSAN PERUBAHAN *(CHANGE MANAGEMENT)*	PERANAN
8.32.2 Panduan Sokongan Perubahan dalam persekitaran produksi contohnya sistem operasi dan pangkalan data, boleh membahayakan integriti dan ketersediaan aplikasi, khususnya pemindahan perisian daripada pembangunan kepada produksi. KKM perlu berhati-hati dengan kesan daripada mengubah perisian dalam persekitaran produksi. Kesan yang tidak dijangka boleh timbul oleh itu, perhatian perlu diberikan sepenuhnya. KKM perlu menjalankan ujian ke atas komponen ICT dalam persekitaran yang selamat serta berasingan daripada persekitaran pembangunan dan persekitaran produksi.	Pemilik Aset Pemilik Sistem Pentadbir Sistem ICT
8.33 MAKLUMAT PENGUJIAN *(TEST INFORMATION)*	**PERANAN**
8.33.1 Perlindungan ke atas Maklumat Ujian Persekitaran pembangunan dan ujian tidak sepatutnya mengandungi maklumat sensitif termasuk data peribadi. Perkara-perkara yang perlu dipertimbangkan dalam melindungi maklumat ujian daripada kehilangan kerahsiaan dan integriti adalah seperti berikut: (a) persekitaran ujian perlu melaksanakan kawalan capaian yang digunakan dalam persekitaran sebenar; (b) penyalinan maklumat sebenar ke dalam persekitaran ujian memerlukan prosedur kebenaran yang berasingan; (c) untuk mengekalkan jejak audit, semua aktiviti yang berkaitan dengan penyalinan, penggunaan dan penyimpanan maklumat sensitif dalam persekitaran ujian hendaklah direkodkan; (d) persekitaran ujian perlu melindungi maklumat sensitif dengan kawalan yang sesuai, seperti penutupan data atau penyingkiran data jika maklumat sensitif ingin digunakan; dan (e) untuk menghapuskan risiko capaian tanpa kebenaran, maklumat yang digunakan dalam persekitaran ujian hendaklah dipindahkan dengan selamat dan dihapuskan mengikut kawalan yang sesuai selepas ujian selesai.	Pemilik Sistem
8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PENGUJIAN AUDIT *(PROTECTION OF INFORMATION SYSTEMS DURING AUDIT TESTING)*	**PERANAN**
8.34.1 Kawalan Audit Sistem Maklumat Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas fungsi penyampaian perkhidmatan. Perkara yang perlu dipertimbangkan adalah seperti berikut: (a) bersetuju dengan permintaan audit untuk mencapai kepada sistem dan data dengan pengurusan yang sesuai; (b) bersetuju dan mengawal skop ujian audit teknikal;	Pemilik Sistem

8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PENGUJIAN AUDIT *(PROTECTION OF INFORMATION SYSTEMS DURING AUDIT TESTING)*	PERANAN
8.34.1 Kawalan Audit Sistem Maklumat Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas fungsi penyampaian perkhidmatan. Perkara yang perlu dipertimbangkan adalah seperti berikut: (a) bersetuju dengan permintaan audit untuk mencapai kepada sistem dan data dengan pengurusan yang sesuai; (b) bersetuju dan mengawal skop ujian audit teknikal; (c) menghadkan ujian audit kepada capaian baca sahaja kepada perisian dan data. Jika capaian baca sahaja tidak tersedia untuk mendapatkan maklumat yang diperlukan, melaksanakan ujian oleh pentadbir berpengalaman yang mempunyai hak capaian yang diperlukan bagi pihak juruaudit; (d) jika capaian diberikan, mewujudkan dan mengesahkan keperluan keselamatan peranti yang digunakan untuk mencapai sistem sebelum membenarkan capaian dibuat; (e) hanya membenarkan capaian selain daripada baca sahaja untuk salinan terpencil fail sistem, menghapuskannya apabila audit selesai, atau memberi mereka perlindungan yang sewajarnya jika terdapat kewajiban untuk menyimpan fail tersebut di bawah keperluan dokumentasi audit; (f) mengenal pasti dan bersetuju dengan permintaan untuk pemprosesan khas atau tambahan, seperti menggunakan alat audit; (g) menjalankan ujian audit yang boleh menjejaskan ketersediaan sistem di luar waktu perkhidmatan; dan (h) memantau dan mengelog semua capaian untuk tujuan audit dan ujian, KKM perlu berhati-hati semasa mengaudit persekitaran ujian atau pembangunan, kerana beberapa risiko, seperti: (a) menjejaskan integriti kod; dan (b) menjejaskan dan kehilangan data sensitif adalah perkara yang serius.	Pemilik Sistem





LAMPIRAN



SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER KEMENTERIAN KESIHATAN MALAYSIA (KKM)

Nama Penuh
(Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan/Gred : .....

Agensi : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber Kementerian Kesihatan Malaysia; dan

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

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....
(Nama Pegawai Keselamatan ICT)
b.p. Ketua Setiausaha
Kementerian Kesihatan Malaysia

Tarikh : .....

PERAKUAN AKTA RAHSIA RASMI 1972 [*AKTA 88*]

PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN PERKHIDMATAN AWAM ATAU YANG BERKHIDMAT DI KEDIAMAN RASMI KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [*Akta 88]* dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan suratan rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesilapan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Saya faham bahawa segala rahsia rasmi dan suratan rasmi yang saya peroleh semasa berurusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan atau menyampaikan, sama ada secara lisan, bertulis atau dengan cara elektronik kepada sesiapa jua dalam apa-apa bentuk, sama ada dalam masa atau selepas berurusan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapatkan kebenaran bertulis daripada pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani satu akuan selanjutnya bagi maksud ini apabila urusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia telah selesai.

Tandatangan : .....

Nama (huruf besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan / Organisasi : .....

Tarikh : .....

Disaksikan oleh : .....
(Tandatangan)

Nama (huruf besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan / Organisasi : .....

Tarikh : .....

Cap Jabatan / Organisasi

PERJANJIAN KERAHSIAAN
(NON-DISCLOSURE AGREEMENT)

BAGI

.....

.....

(Sila lengkapkan nama projek)

Saya .....
(Nyatakan nama penuh mengikut kad pengenalan)

No. Kad Pengenalan ..... dari

.....
(Nyatakan alamat penuh organisasi/syarikat dan lain-lain)

.....

dengan ini:

(a) akan memastikan maklumat yang didedahkan hanyalah untuk tujuan projek tersebut di atas sahaja;

(b) akan memberi perlindungan kerahsiaan yang sewajarnya kepada semua maklumat berkaitan projek ini tanpa mengira bentuk;

(c) tidak mempunyai kepentingan peribadi terhadap maklumat berkaitan projek ini;

(d) tidak akan mendedahkan kepada mana-mana orang atau badan atau entiti, apa-apa maklumat yang didedahkan kepadanya berkaitan projek ini kecuali dengan kebenaran bertulis terlebih dahulu daripada Kementerian Kesihatan Malaysia (KKM); dan

(e) akan menentukan dan mengekalkan langkah-langkah kawalan yang berkesan untuk menjaga kerahsiaan maklumat berkaitan projek daripada pihak yang tidak diberikuasa, penggunaan, salinan atau penyebaran.

Sekiranya saya didapati melanggar mana-mana klausa di bawah perjanjian ini, tindakan undang-undang boleh diambil oleh Kementerian Kesihatan Malaysia (KKM) terhadap saya berdasarkan peruntukan sebarang undang-undang bertulis yang berkuatkuasa dari semasa ke semasa.

Sekian, terima kasih.

.....	.....
(Tandatangan Organisasi/Syarikat)	(Tandatangan Wakil KKM)
.....	.....
(Nama)	(Nama)
.....	.....
(No. Kad Pengenalan)	(No. Kad Pengenalan)
Tarikh:	Tarikh: .....

PERJANJIAN UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI

Polisi ini hendaklah dibaca bersama-sama dengan akta-akta, warta, pekeliling-pekeliling, surat pekeliling dan peraturan dalaman yang berkaitan dan sedang berkuat kuasa seperti berikut:

A. UNDANG-UNDANG MENGENAI KESELAMATAN SIBER DI MALAYSIA

1) Akta Hak Cipta (Pindaan) 1997
2) Akta Jenayah Komputer 1997
3) Akta Tandatangan Digital 1997
4) Akta Teleperubatan 1997
5) Akta Komunikasi dan Multimedia 1998
6) Akta Perdagangan Elektronik 2006
7) Akta Aktiviti Kerajaan Elektronik 2007
8) Akta Perlindungan Data Peribadi 2010
9) Akta Keselamatan Siber 2024

B. PEKELILING DAN GARIS PANDUAN KERAJAAN MENGENAI KESELAMATAN SIBER

1) *Malaysian Public Sector Management of Information and Communications Technology Security Handbooks* (MyMIS) bertarikh 15 Januari 2002
2) Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian *Government Computer Emergency Response Team* (GCERT) Oleh Agensi Keselamatan Siber Negara (NACSA) bertarikh 28 Januari 2019
3) Surat Ketua Pengarah Keselamatan Negara, Majlis Keselamatan Negara – Pengurusan Maklumat Pegawai Keselamatan ICT (ICTSO) Sektor Awam bertarikh 28 Februari 2019
4) Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan Dan Pengendalian
5) Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024
6) Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024
7) Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)
8) Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024
9) Surat Pekeliling Am Bilangan 8 Tahun 2024 - Garis Panduan Pengurusan Dan Pengendalian Rahsia Rasmi Dalam Perkhidmatan Awam
10) PKPA Bil. 1 Tahun 2021 adalah Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam

C. DASAR DAN PERATURAN CHIEF GOVERNMENT SECURITY OFFICER (CGSO)

1) Akta Rahsia Rasmi 1972 (Akta 88)

2) Akta Kawasan Larangan dan Tempat Larangan (Akta 298)

3) Arahan Keselamatan (Semakan dan Pindaan 2017)

D. AKTA ARKIB NEGARA MALAYSIA

1) Akta Arkib Negara 2003 [Akta 629]

2) Akta Arkib

E. AKTA, PERATURAN DAN PERINTAH AM (JPA)

1) Perintah-Perintah Am

F. PEKELILING KEMAJUAN PENTADBIRAN AWAM – JABATAN DIGITAL NEGARA (JDN)

1) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan
2) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021 – Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam (dikeluarkan oleh JDN pada 10 Jun 2021)

G. ARAHAN / SURAT PEKELILING / SURAT ARAHAN – JABATAN DIGITAL NEGARA (JDN)

1) Surat Arahan Ketua Setiausaha Negara – Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-agensi Kerajaan bertarikh 20 Oktober 2006
2) Arahan Teknologi Maklumat 2007
3) Surat Arahan Ketua Pengarah MAMPU – Langkah-langkah Mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan bertarikh 1 Jun 2007
4) Surat Arahan Ketua Pengarah MAMPU – Langkah-langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-agensi Kerajaan bertarikh 23 November 2007
5) Surat Arahan Ketua Pengarah MAMPU – “Pelaksanaan Blog Bagi Agensi Sektor Awam” bertarikh 17 Julai 2009
6) Surat Ketua Pengarah MAMPU – "Penggunaan Media Jaringan Sosial Di Sektor Awam" bertarikh 19 November 2009
7) Surat Arahan Ketua Pengarah MAMPU Tahun 2010 – Pemantapan Penggunaan Dan Pengurusan E-mel Di Agensi-Agensi Kerajaan
8) Surat Arahan Ketua Pengarah MAMPU – “Amalan Terbaik Penggunaan Media Jaringan Sosial Di Sektor Awam” bertarikh 8 April 2011
9) Surat Pekeliling Am Bilangan 2 Tahun 2021 – Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam
10) Garis Panduan Pengurusan Kesinambungan Perkhidmatan dalam Perkhidmatan Awam (Business Continuity Management) seperti yang ditetapkan oleh Garis Panduan Bil. 1 2025

H. ARAHAN DAN PEKELILING PERBENDAHARAAN

1) Pekeliling Perbendaharaan Malaysia – Am 2.1 Tatacara Pengurusan Aset Alih Kerajaan
2) Pekeliling Perbendaharaan Malaysia – PK 2.1 Kaedah Perolehan Kerajaan
3) Pekeliling Perbendaharaan Malaysia – PS 2.2 Terimaan Kerajaan Secara Elektronik Melalui Portal Kementerian atau Jabatan
4) Pekeliling Perbendaharaan – PK 2.6 Perolehan Perkhidmatan Pengkomputeran Awan (Cloud) Sektor Awam berkuatkuasa mulai 15 April 2022
5) Arahan Perbendaharaan (Pindaan 2023)

I. GARIS PANDUAN / PEKELILING / SURAT PEKELILING – KEMENTERIAN KESIHATAN MALAYSIA (KKM)

1) Pekeliling Ketua Pengarah Kesihatan Bil 16/2010 – Garis Panduan Penyediaan Laporan Perubatan Di Hospital-Hospital Dan Institusi Perubatan Kementerian Kesihatan Malaysia
2) Garis Panduan User Access Control Policy (UACP), Kementerian Kesihatan Malaysia Tahun 2011
3) Surat Pekeliling Am Kementerian Kesihatan Malaysia Bil 1 Tahun 2016 – Tatacara Pelaksanaan Projek ICT Di Kementerian Kesihatan Malaysia (KKM)
4) Surat Pekeliling Am Kementerian Kesihatan Malaysia Bil 2 Tahun 2016 – Garis Panduan Kesediaan Infrastruktur Teknologi Maklumat Dan Komunikasi (ICT) Di Agensi Dan Fasiliti Kementerian Kesihatan Malaysia (KKM)
5) Surat Pekeliling Ketua Pengarah Kesihatan Bil 5/2023 – Garis Panduan Pengendalian dan Pengurusan Rekod Perubatan Pesakit Di Fasiliti Kementerian Kesihatan Malaysia

J. AM

1) Standard Operating Procedure (SOP) ICT

KEMENTERIAN KESIHATAN MALAYSIA

SIDANG REDAKSI

POLISI KESELAMATAN SIBER

BAHAGIAN PENGURUSAN MAKLUMAT

PENAUNG

Pn. Rohayati Binti Ramli
Setiausaha Bahagian
Bahagian Pengurusan Maklumat, KKM

PENGERUSI

Pn. Mahani Binti Saron
Timbalan Setiausaha Bahagian
Bahagian Pengurusan Maklumat, KKM

PENASIHAT

Ts. Siti Aini Binti Abdul Manan
Ketua Penolong Setiausaha
Bahagian Pengurusan Maklumat, KKM

KETUA EDITOR

En. Muhammad Nasri Bin Mohd Amin
Penolong Setiausaha Kanan
Bahagian Pengurusan Maklumat, KKM

PENYELARAS

Pn. Rusmiza Binti Kadir
Pn. Nurul Hanis Binti Rusnan
Pn. Norfazira Binti Abdullah

...dan terima kasih kepada lain-lain pegawai yang terlibat secara langsung dan tidak langsung dalam penghasilan buku ini.

KUMPULAN INPUT TEKNIKAL

Ts. Dr. Cecilia Adrian
Pn. Siti Norbaya Binti Shaharul Anwar
En. Mohamad Fadzlan Bin Yaacob
En. Muslin Yin
En. Mohd Rafizam Bin Mohamed
Ts. Asnida Akmal Noor Binti Che Ahmad
Pn. Siti Zaileha Bin A Salam
Pn. Nurzakina Binti Zakaria
Pn. Subashini A/p Panchanathan
Pn. Rohaya Binti Yahaya
Pn. Faraliza Binti Md. Salleh
Ts. Mohd Fittri Aziz Bin Mohd Alias
Pn. Rusmawati Binti Ishak
Pn. Nurul Fateen Binti Yahya
Pn. Nurhanan Binti Ahmad
En. Farouk Bin Abdul Jalin @ Abd Jalil
Pn. Yunura Azura Binti Yunus
Pn. Nur Diyana Binti Fazlollah Suhaimi
En. Azizi Bin Zulkipli
En. Amir Fakhri Bin Badrul Azman
Ts. Albert Peter Jaua
En. Mohamad Zakie Bin Shafie
En. Masnizar Bin Jamian
En. Mohd Zarki Bin Jaafar
En. Hamidee Bin Harun
En. Gobibaskaran Govindaraju
Pn. Noor Iswana Binti Hj Ahmad
Pn. Nurul Salwa Binti Abdul Muluk
En. Fizalyhan Bin Sadie





KEMENTERIAN KESIHATAN MALAYSIA

Kementerian Kesihatan Malaysia
Blok E1, E3, E6, E7 & E10, Kompleks E
Pusat Pentadbiran Kerajaan Persekutuan
62590 Putrajaya, Malaysia.

Tel: 03-8883 3883
E-mel: sec@moh.gov.my
Portal: www.moh.gov.my

Kementerian Kesihatan Malaysia

@KKMPutrajaya

kementeriankesihatanmalaysia

Kementerian Kesihatan Malaysia

kkmputrajaya

ISBN 978-967-2469-83-4

