KEMENTERIAN PERLADANGAN
DAN KOMODITI

POLISI
KESELAMATAN
SIBER

VERSI
1.0

Kementerian Perladangan dan Komoditi

POLISI KESELAMATAN SIBER

Versi 1.0

KEMENTERIAN PERLADANGAN DAN KOMODITI (KPK)

BAHAGIAN PENGURUSAN MAKLUMAT (BPM)

POLISI KESELAMATAN SIBER VERSI 1.0
KEMENTERIAN PERLADANGAN DAN KOMODITI
(PKS KPK VERSI 1.0)

ISBN 978-967-19545-9-1
9 7 8 9 6 7 1 9 5 4 5 9 1
POLISI KESELAMATAN SIBER VERSI 1.0 KEMENTERIAN PERLADANGAN DAN KOMODITI

e-Book

Diterbitkan oleh:
Kementerian Perladangan dan Komoditi (KPK)
No. 15, Aras 6-13,
Persiaran Perdana Presint 2,
62654, Putrajaya, MALAYSIA

SEJARAH DOKUMEN

Tarikh	Versi	Kelulusan	Tarikh Kuatkuasa
11 Mac 2010	DKICT 1.0	JPICT Bil. 1/2010	11 Mac 2010
21 Oktober 2013	DKICT 2.0	Pengurusan KPK Bil. 11/2013	21 Oktober 2013
6 Ogos 2018	DKICT 3.0	JPICT Bil. 2/2018	6 Ogos 2018
19 Disember 2022	PKS 1.0	JPICT Bil. 4/2022	19 Disember 2022

SEJARAH PINDAAN

Tarikh	Versi	Butiran Pindaan
3 Mac 2015	DKICT 2.0	Pindaan terhadap perkara 020103 Pegawai Keselamatan ICT (ICTSO) bagi MPI ialah KPSU (BPM), KPK
24 April 2018	DKICT 3.0	Penambahan perkara 030203, 030204, 030205, 030206 dan 030207 iaitu Keselamatan Rahsia Rasmi Dalam Persekitaran Teknologi Maklumat dan Komunikasi (ICT).
3 Ogos 2018	DKICT 3.0	Pindaan terhadap perkara 070301 c) “Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus”.
14 Oktober 2022	PKS 1.0	Penggantian dokumen Dasar Keselamatan ICT (DKICT) kepada Polisi Keselamatan Siber (PKS)

ISI KANDUNGAN

PENGENALAN

Polisi Keselamatan Siber (PKS) Kementerian Perladangan dan Komoditi (KPK) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT) di KPK. Polisi ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT KPK.

OBJEKTIF

Polisi Keselamatan Siber KPK diwujudkan untuk menjamin kesinambungan perkhidmatan KPK dengan meminimumkan kesan insiden keselamatan siber.

Polisi ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi KPK. Ia hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Manakala, objektif utama keselamatan siber KPK ialah seperti berikut:

a) Memastikan kelancaran operasi KPK dan meminimumkan kerosakan atau kemusnahan;

b) Melindungi kepentingan pihak-pihak yang terikat dengan sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;

c) Memperkemaskan Pengurusan risiko; dan

Mencegah salah guna atau kecurian aset ICT KPK.

PERNYATAAN POLISI

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

Keselamatan siber adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan siber berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan siber iaitu:

a) Melindungi maklumat rahsia rasmi dan maklumat rasmi KPK dari capaian tanpa kuasa yang sah;

b) Menjamin setiap maklumat adalah tepat dan sahih;

c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

PKS KPK merangkumi perlindungan ke atas semua bentuk maklumat elektronik yang bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehcapaian kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

a) **Kerahsiaan** - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

b) **Integriti** - Data dan maklumat hendaklah tepat, lengkap dan sentiasa dikemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan;

c) **Tidak Boleh Disangkal** - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

d) **Kesahihan** - Data dan maklumat hendaklah dijamin kesahihannya; dan

e) **Ketersediaan** - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP

Sistem ICT KPK terdiri daripada organisasi, manusia, perkakasan, perisian, telekomunikasi, Perkhidmatan/kemudahan ICT, data dan maklumat. Polisi Keselamatan Siber KPK menetapkan keperluan-keperluan asas berikut:

a) Data dan maklumat termasuk *hardcopy* dan *softcopy* hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan

b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan KPK, perkhidmatan dan pelanggan.

Bagi menentukan Sistem ICT ini terjamin keselamatannya sepanjang masa, PKS KPK ini merangkumi perlindungan semua bentuk maklumat ICT KPK yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

a) Data dan maklumat

Semua data dan maklumat yang disimpan atau digunakan di pelbagai media atau peralatan ICT.

b) Perkakasan/Peralatan ICT

Semua peralatan komputer dan peripheral seperti server, firewall, komputer peribadi, stesen Kerja, kerangka utama, pencetak, peralatan multimedia dan alat-alat prasarana seperti Uninterruptible Power Supply (UPS), punca kuasa dan lain-lain.

c) Perisian

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

d) Media Storan

Semua media storan yang digunakan untuk menyimpan data dan maklumat seperti optical disk, flash disk, hard disk, USB flash disk dan lain-lain.

e) Media Komunikasi

Semua peralatan berkaitan komunikasi seperti pelayan (server) atau peralatan rangkaian, gateway, router, peralatan PABX, wireless LAN, Talian ISDN, peralatan video conferencing, modem, kabel rangkaian, Network Interface Card (NIC), switch dan sebagainya

f) Dokumentasi

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

g) Manusia

Semua pengguna yang dibenarkan. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

h) Premis Komputer Dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a) - (f) di atas.

i) Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsinya seperti:

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem sekatan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, pendingin hawa, sistem pencegah kebakaran dan lain-lain.

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

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada PKS KPK dan perlu dipatuhi adalah seperti berikut:

a) Akses atas dasar perlu mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut.

b) Hak akses minimum

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

c) Kebertanggungjawaban atau Akauntabiliti

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

d) Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

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

iii. Menentukan maklumat sedia untuk digunakan;

iv. Menjaga kerahsiaan kata laluan;

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

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

vii. Menjaga kerahsiaan langkah-langkah keselamatan siber dari diketahui umum.

e) Pengasingan

Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

f) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

Dengan itu, aset ICT seperti komputer, pelayan, router, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*.

g) Pematuhan

PKS KPK hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan siber;

h) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/ kesinambungan perkhidmatan; dan

i) Saling Bergantung

Setiap prinsip di atas adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan

dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

PENILAIAN RISIKO KESELAMATAN SIBER

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

KPK hendaklah melaksanakan penilaian risiko keselamatan siber secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan siber. Seterusnya mengambil tindakan susulan dan langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan siber berdasarkan penemuan penilaian risiko.

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

KPK bertanggungjawab melaksanakan dan menguruskan risiko keselamatan siber selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam. KPK perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

b) Menerima dan bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;

c) Mengelak dan mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan mencegah berlakunya risiko; dan

d) Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

KAWALAN
01

POLISI KESELAMATAN MAKLUMAT

KAWALAN 01
POLISI KESELAMATAN MAKLUMAT

OBJEKTIF

PKS KPK ini diwujudkan untuk melindungi aset ICT KPK bagi memastikan kelancaran pengoperasian Kementerian secara berterusan, meminimumkan kerosakan atau kemusnahan aset-aset ICT melalui usaha pencegahan atau mengurangkan kesan kejadian yang tidak diingini berdasarkan kepada ciri-ciri keselamatan iaitu kerahsiaan, *integriti*, tidak boleh disangkal, kebolehsediaan dan kesahihan.

K01/01 Pelaksanaan Dasar	Tindakan
Pelaksanaan dasar ini akan dijalankan oleh Ketua Setiausaha (KSU) KPK dan dibantu oleh Jawatankuasa Pemandu ICT KPK yang terdiri dari Timbalan Ketua Setiausaha (Perancangan Strategik dan Pengurusan) selaku CIO/CDO, semua Setiausaha Bahagian dan Ketua Unit serta Pegawai Keselamatan ICT (ICTSO).	KSU

K01/02 Penyebaran Dasar	Tindakan
Dasar ini hendaklah disebarkan dan dipatuhi oleh semua pengguna aset ICT KPK termasuk kontraktor dan pihak ketiga yang berurusan atau memberikan perkhidmatan ICT kepada KPK.	ICTSO

K01/03 Penyelenggaraan Dasar	Tindakan
Dasar ini hendaklah disemak dan dipinda mengikut keperluan selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Prosedur yang perlu berhubung penyelenggaraan PKS KPK ialah : i. mengenal pasti dan menentukan perubahan yang diperlukan; ii. mendapatkan kelulusan JPICT; iii. memaklumkan pindaan yang telah disahkan oleh JPICT kepada semua pengguna; dan iv. menyemak semula dokumen sekurang-kurangnya sekali setahun atau mengikut keperluan bagi memastikan dokumen sentiasa relevan.	ICTSO

K01/04 Pematuhan Dasar	Tindakan
PKS KPK ini mestilah dipatuhi oleh semua pengguna ICT KPK dan tiada sebarang pengecualian diberikan.	Semua

KAWALAN
02

ORGANISASI KESELAMATAN MAKLUMAT

KAWALAN 02
ORGANISASI KESELAMATAN MAKLUMAT

OBJEKTIF

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber KPK.

K02/01 ORGANISASI KESELAMATAN KPK

K02/01/01 Ketua Setiausaha (KSU) KPK	Tindakan
KSU KPK adalah berperanan dan bertanggungjawab dalam perkara-perkara berikut: a) Menetapkan arah tuju dan strategi untuk pelaksanaan keselamatan siber KPK dan semua Agensi di bawahnya; b) Memperuntukkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju dan strategik keselamatan siber KPK dan semua Agensi di bawahnya; c) Memastikan semua pengguna mematuhi Polisi Keselamatan Siber KPK; d) Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KPK; dan e) Melantik CIO/CDO dan ICTSO serta memaklumkan pelantikan kepada NACSA .	KSU

K02/01/02 Ketua Pegawai Maklumat (CIO/CDO)	Tindakan
Ketua Pegawai Maklumat (CIO/CDO) bagi KPK ialah Timbalan Ketua Setiausaha (Perancangan Strategik dan Pengurusan), KPK. Peranan dan tanggungjawab CIO/CDO adalah seperti berikut: a) Membantu KSU dalam melaksanakan tugas-tugas yang melibatkan ICT dan keselamatan siber; b) Meluluskan semua prosedur, standard, dan garis panduan keselamatan siber KPK;	CIO/CDO

c) Meluluskan perlaksanaan atau aktiviti keselamatan siber KPK;

d) Meluluskan pelan latihan dan program kesedaran keselamatan siber seperti penyediaan PKS KPK serta pengurusan risiko dan pengauditan; dan

K02/01/03 Pengurus ICT	Tindakan
Pengurus ICT bagi KPK ialah Setiausaha Bahagian (SUB), Bahagian Pengurusan Maklumat KPK.	SUB BPM

Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:

a) Mengkaji, menguji dan melaksanakan kawalan keselamatan siber selaras dengan keperluan KPK;

b) Membuat penilaian keberkesanan kawalan keselamatan siber;

c) Meluluskan prosedur teknikal perlaksanaan kawalan keselamatan;

d) Menentukan kawalan akses pengguna terhadap aset ICT KPK;

e) Memastikan semua Polisi Keselamatan Siber di patuhi;

f) Berperanan sebagai Pengarah *Cyber Security Incident Response Team* (CSIRT) KPK.

g) Mengambil tindakan terhadap pencerobohan, ancaman atau penemuan mengenai kelemahan keselamatan siber; dan

h) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan siber KPK.

K02/01/04 Pegawai Keselamatan ICT (ICTSO)	Tindakan
Pegawai Keselamatan ICT (ICTSO) bagi KPK ialah Ketua Penolong Setiausaha (KPSU), Bahagian Pengurusan Maklumat, KPK. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a) Mengurus keseluruhan program-program keselamatan siber KPK; b) Memberi penerangan dan pendedahan berkenaan Polisi Keselamatan Siber KPK kepada semua pengguna; c) Menguatkuasakan pelaksanaan Polisi Keselamatan SIber (PKS) KPK; d) Menjalankan pengurusan risiko dan audit keselamatan siber berpandukan rangka kerja, polisi, pekeliling, garis panduan dan pelan pengurusan keselamatan maklumat yang sedang berkuat kuasa; e) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi Keselamatan Siber KPK; f) Menyediakan dan menyebarkan amaran terhadap kemungkinan berlakunya ancaman keselamatan siber dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; g) Berperanan sebagai Pengurus *Cyber Security Incident Response Team* (CSIRT) KPK; h) Melaporkan insiden keselamatan siber kepada NC4, NACSA dan memaklumkan kepada CDO; i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera;	**ICTSO**

j) Melaksanakan dan memantau pematuhan Polisi Keselamatan Siber (PKS) oleh warga KPK, pihak pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPK;

k) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber;

l) Menyedia dan merangka latihan dan program kesedaran keselamatan siber; dan

m) Menjalankan penilaian tahap keselamatan siber dan mengambil tindakan pengukuhan bagi meningkatkan tahap keselamatan siber supaya insiden sama tidak berulang.

K02/01/05 Pentadbir Sistem ICT	Tindakan
Pentadbir Sistem ICT bagi KPK ialah Penolong Setiausaha (PSU) ICT yang dilantik untuk mentadbir dan menguruskan sistem-sistem ICT. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: a) Pentadbir Rangkaian dan Keselamatan; b) Pentadbir Pangkalan Data; c) Pentadbir Laman Web (*Web Master*); d) Pentadbir Pusat Data (*Server Farm*); e) Semua Pentadbir Sistem Aplikasi; f) Pentadbir E-mel; dan g) Pegawai Aset ICT	**Pentadbir Sistem ICT**

K02/01/06 Pentadbir Rangkaian dan Keselamatan	Tindakan
Peranan dan tanggungjawab Pentadbir Rangkaian Dan Keselamatan adalah seperti berikut: a) memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di KPK beroperasi sepanjang masa; b) memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna;	**Pentadbiran Rangkaian dan Keselamatan**

c) merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada;
d) mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil;
e) melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT;
f) memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian KPK secara tidak sah seperti melalui peralatan modem dan *dial-up*;
g) menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian;
h) memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; dan
i) memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa.

K02/01/07 Pentadbir Pangkalan Data	**Tindakan**

Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut:

Pentadbir Pangkalan Data

a) melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data;
b) memastikan pangkalan data boleh digunakan pada setiap masa;
c) melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data;
d) memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur;
e) melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip PKS;
f) melaksanakan proses perkemasan data (housekeeping) di dalam pangkalan data; dan
g) melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.

K02/01/08 Pentadbir Laman Web KPK (*Web Master*)	Tindakan
Peranan dan tanggungjawab Pentadbir Laman Web KPK adalah seperti berikut: a) menerima kandungan Laman Web KPK yang telah disahkan kesahihan dan terkini daripada sumber yang sah; b) memantau prestasi capaian dan menjalankan ujian penalaan (*tuning*) prestasi untuk memastikan akses yang lancar; c) memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai antara muka Laman Web KPK; d) mengasingkan kandungan dan aplikasi dalam talian untuk capaian secara *Intranet* dan *Internet*; e) memastikan hanya maklumat yang bersifat terbuka dipaparkan di Laman Web KPK; f) memastikan reka bentuk Laman Web KPK dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; g) melaksanakan perkemasan keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di *web server*; h) memantau proses *backup* dan *restoration* ke atas kandungan Laman Web KPK dan sistem aplikasi; dan i) melaporkan sebarang pelanggaran keselamatan Laman Web KPK kepada ICTSO.	**Pentadbir Laman Web KPK (Web Master)**

K02/01/09 Pentadbir Pusat Data (*Server Farm*)	Tindakan
Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti berikut: a) memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat; b) memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data; c) menjadualkan dan melaksanakan proses backup dan restoration ke atas pangkalan data dan sistem secara berkala; d) menyediakan perancangan PKP dalam PKS; e) melaksanakan prinsip-prinsip PKS;	Pentadbir Pusat Data (Server Farm)

f) memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan;
g) melaporkan sebarang pelanggaran keselamatan Pusat Data KPK kepada ICTSO; dan
h) memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa.

K02/01/10 Semua Pentadbir Sistem Aplikasi	Tindakan

Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut:

Semua Pentadbir Sistem Aplikasi

a) mengkaji cadangan pembangunan atau penyelarasan sistem atau modul di KPK;
b) membuat kajian semula serta memperbaiki sistem atau modul sedia ada di KPK;
c) membuat pertimbangan dan mengusulkan cadangan pelaksanaan sistem atau modul di KPK;
d) membuat pemantauan dan penyelenggaraan terhadap sistem atau modul dari semasa ke semasa;
e) bertanggungjawab dalam aspek-aspek pelaksanaan keseluruhan sistem atau modul;
f) menyediakan dokumentasi sistem atau modul dan manual pengguna;
g) memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas;
h) memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya;
i) memastikan *virus pattern*, *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi dikemaskini supaya terhindar daripada ancaman virus dan penggodam;
j) mematuhi dan melaksanakan prinsip-prinsip PKS dalam pewujudan akaun pengguna ke atas setiap sistem aplikasi;
k) mengehadkan capaian Dokumentasi Sistem Aplikasi bagi mengelakkan dari penyalahgunaannya; dan
l) melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya.

K02/01/11 Pentadbir E-mel	Tindakan

Peranan dan tanggungjawab Pentadbir E-mel adalah seperti berikut:

Pentadbir E-mel

a) menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat;
b) pentadbir e-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib;
c) memastikan pengguna e-mel KPK berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel KPK dan Internet KPK
d) serta pelaksanaan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan.
e) memastikan kemudahan membuat capaian e-mel melalui pelbagai peralatan ICT dan alat komunikasi;
f) mengesah dan memaklumkan kepada ICTSO sekiranya mengalami insiden keselamatan melalui saluran rasmi; dan
g) memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa.

K02/01/12 Pegawai Aset ICT	Tindakan

Pegawai Aset ICT ialah pegawai yang dilantik oleh Pegawai Pengawal. Peranan dan tanggungjawab Pegawai Aset ICT adalah seperti berikut:

Pegawai Aset ICT

h) memastikan pengurusan aset ICT Kerajaan dijalankan selaras dengan peraturan yang ditetapkan;
i) memastikan penerimaan aset ICT Kerajaan dilaksanakan oleh pegawai yang dilantik oleh Ketua Jabatan/ Bahagian;
j) memastikan semua aset ICT Kerajaan yang diterima, didaftarkan menggunakan Sistem Pemantauan Pengurusan Aset (SPA) dalam tempoh dua (2) minggu dari tarikh pengesahan penerimaan aset;

k) memastikan semua aset ICT Kerajaan yang dipinjam, direkodkan ke dalam Rekod Pergerakan Aset. Aset tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan secara bertulis daripada Ketua Jabatan/ Pegawai Aset/ Pegawai-pegawai lain yang diberi kuasa oleh Ketua Jabatan;
l) memastikan Daftar Aset ICT dikemas kini apabila berlaku penambahan/ penggantian/ naik-taraf aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira;
m) memastikan semua aset ICT Kerajaan diberi tanda pengenalan dengan cara melabel tanda Hak Kerajaan Malaysia dan nama KPK/Bahagian berkenaan di tempat yang mudah dilihat dan sesuai pada aset berkenaan;
n) memastikan semua aset ICT Kerajaan ditandakan dengan Nombor Siri Pendaftaran mengikut susunan yang ditetapkan;
o) memastikan senarai daftar induk aset ICT Kerajaan disediakan;
p) memastikan senarai aset ICT Kerajaan disediakan mengikut lokasi dan format Senarai Aset ICT Kerajaan dalam dua (2) buah salinan. Satu (1) senarai berkenaan perlu disimpan oleh Pegawai Aset ICT/ Pembantu Pegawai Aset ICT dan satu (1) salinan perlu dipaparkan oleh pegawai yang bertanggungjawab di lokasi;
q) memastikan setiap kerosakan aset ICT Kerajaan dilaporkan untuk tujuan penyelenggaraan; dan
r) bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset ICT Kerajaan.

K02/01/13 Pengguna	**Tindakan**
Pengguna adalah pegawai-pegawai yang dilantik oleh KPK secara tetap, kontrak dan sambilan juga pihak luaran yang terlibat dalam penggunaan atau capaian kepada aset dan Perkhidmatan ICT Kementerian.	
Pengguna mempunyai peranan dan tanggung-jawab seperti berikut:	**Semua Pengguna**
a) Membaca, memahami dan mematuhi PKS KPK;	

b) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya;

c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat;

d) Melaksanakan prinsip-prinsip PKS KPK dan menjaga kerahsiaan maklumat KPK;

e) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera;

f) Menghadiri program-program kesedaran mengenai keselamatan siber; dan

g) Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber (PKS) KPK sebagaimana di **LAMPIRAN 1**.

K02/01/14 Jawatankuasa Keselamatan ICT (JKKICT) KPK	**Tindakan**

Jawatankuasa Keselamatan ICT (JKKICT) adalah jawatankuasa yang bertanggung-jawab ke atas segala perancangan, pelaksanaan, pemantauan dan strategi keselamatan siber KPK. Mesyuarat perlu diadakan sekurang-kurangnya sekali (1) setahun.

Di KPK, Jawatankuasa Pemandu ICT (JPICT) atau Mesyuarat Pengurusan juga berperanan sebagai JKKICT KPK.

Keanggotaan JKKICT KPK adalah seperti berikut:

a) Pengerusi : KSU KPK

b) Ahli:

i. Timbalan Ketua Setiausaha
ii. Ketua Pegawai Maklumat (CIO)
iii. Semua Setiausaha Bahagian dan Ketua Unit atau wakil
iv. ICTSO

c) Urus Setia bagi JKKICT KPK ialah Urusetia JPICT/Jawatankuasa Kerja ISMS KPK.

d) Bidang Kuasa:

i. Memperakui/meluluskan dokumen Polisi Keselamatan Siber KPK;
ii. Meluluskan tahap pematuhan keselamatan siber;
iii. Meluluskan teknologi yang bersesuaian untuk dilaksanakan di dalam memperkukuhkan keselamatan KPK;
iv. Meluluskan cadangan penyelesaian terhadap keperluan keselamatan siber;
v. Memastikan Polisi Keselamatan Siber KPK selaras dengan dasar-dasar ICT kerajaan semasa;
vi. Meluluskan laporan dan membincangkan hal-hal keselamatan siber semasa;
vii. Meluluskan tindakan yang melibatkan pelanggaran PKS KPK; dan
viii. Meluluskan tindakan yang perlu diambil mengenai sebarang insiden.

JKKICT

K02/01/15 Jawatankuasa Pemandu ICT (JPICT) KPK	**Tindakan**

Jawatankuasa Pemandu ICT (JPICT) adalah jawatankuasa yang bertanggung-jawab ke atas segala perancangan, pelaksanaan, pemantauan dan strategi pelaksanaan ICT di KPK. Mesyuarat perlu diadakan empat (4) kali setahun.

Keanggotaan JPICT KPK adalah seperti berikut:

a) Pengerusi : KSU KPK

b) Ahli:

i. Timbalan Ketua Setiausaha
ii. Ketua Pegawai Maklumat (CIO)
iii. Semua Setiausaha Bahagian dan Ketua Unit atau wakil
iv. ICTSO

JPICT

c) Urus Setia bagi JPICT KPK ialah Bahagian Pengurusan Maklumat (BPM) KPK.

d) Bidang kuasa:

i. menetapkan arah tuju dan strategi ICT untuk pelaksanaan ICT di KPK;
ii. merancang, menyelaras dan memantau pelaksanaan program atau projek ICT KPK;
iii. menyelaras dan menyeragamkan pelaksanaan ICT agar selari dengan Pelan Strategik Pendigitalan KPK dan Pelan Strategik Pendigitalan Sektor Awam ;
iv. meluluskan projek-projek ICT KPK dan Agensi-agensi di bawah KPK;
v. mengikuti dan memantau perkembangan program ICT serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT di KPK;
vi. merancang dan menentukan langkah-langkah keselamatan siber di KPK;
vii. mengemukakan perolehan ICT yang telah diluluskan di peringkat JPICT KPK kepada Jawatankuasa Teknikal ICT Sektor Awam (JTISA) di bawah MAMPU untuk kelulusan;
viii. mengemukakan laporan kemajuan projek ICT yang diluluskan kepada MAMPU melalui Sistem PROFIT.

K02/01/16 Cyber Security Incident Response Team (CSIRT) KPK	**Tindakan**

Pengguna wajib melaporkan sebarang insiden ICT kepada *Cyber Security Incident Response Team* (CSIRT) KPK mengikut prosedur yang ditetapkan apabila berlaku insiden yang menjejaskan keselamatan siber.

CSIRT KPK adalah pasukan yang akan bertindak semasa berlaku insiden keselamatan siber di KPK.

Peranan dan tanggungjawab CSIRT adalah seperti berikut :

a) Memantau, mengesan insiden, menerima, dan mengesahkan aduan insiden keselamatan siber, seterusnya mengenal pasti jenis insiden serta menilai impak insiden keselamatan siber;

b) Merekod dan menjalankan siasatan awal terhadap insiden yang diterima;
c) Melaksanakan pengurusan dan pengendalian insiden keselamatan siber serta mengambil tindakan awal pemulihan;
d) Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan serta pengukuhan keselamatan siber supaya insiden baharu dapat dielakkan;
e) Melaporkan insiden keselamatan siber kepada NC4 serta memaklumkan kepada CDO;
f) Menasihat semua Bahagian dan Agensi di bawah KPK mengambil tindakan pemulihan dan pengukuhan.
g) Menyebarkan makluman/amaran berkaitan insiden kepada semua Bahagian dan Agensi di bawah KPK.
h) Memastikan fail log disimpan sekurang-kurangnya enam bulan di tempat yang selamat.

Pasukan CSIRT KPK

K02/01/17 Jawatankuasa Pelan Pemulihan Bencana (JKDRP)	Tindakan

Keanggotaan JKDRP BPM adalah seperti berikut:

a) Pengerusi: SUB BPM
b) Ahli:
   i. Pasukan Pengurusan Bencana ;
   ii. Pasukan Sistem dan Operasi Pusat Data;
   iii. Pasukan Rangkaian dan Keselamatan;
   iv. Pasukan Aplikasi;
   v. Pasukan Pangkalan Data; dan
   vi. Pasukan Meja Bantuan.
c) Urus setia: BPM
d) Bidang kuasa:
   i. membangunkan Dokumen Pelan Pemulihan Bencana (DRP);
   ii. menyediakan kemudahan pemulihan bencana atau Pusat Pemulihan Bencana (*Disaster Recovery Centre*);
   iii. membuat penilaian ke atas masalah dan jangkaan akibat bencana;

JKDRP

iv. memaklumkan pengurusan atasan berkenaan bencana, kemajuan pemulihan bencana dan masalah;
v. mengaktifkan prosedur pemulihan bencana;
vi. mengkoordinasi operasi pemulihan;
vii. memantau operasi pemulihan dan memastikan jadual pemulihan dipatuhi;
viii. mendokumentasikan operasi pemulihan; dan
ix. mengkoordinasi simulasi pemulihan bencana.

K02/02 PIHAK KETIGA/PIHAK LUARAN

K02/02/01 Keperluan Keselamatan Siber di dalam Kontrak dengan Pihak Ketiga	Tindakan
Pihak Ketiga/ Pihak Luaran terdiri daripada pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT JKPPK atau pelawat yang mengunjungi KPK atas urusan rasmi.	
Perjanjian kontrak dengan pihak ketiga / pihak luaran yang berurusan dengan aset ICT KPK adalah perlu bagi memastikan penggunaan maklumat dan kemudahan prosesan maklumat dikawal.	
Perkara yang perlu dipatuhi di dalam perjanjian adalah seperti berikut:	
a) Membaca, memahami dan mematuhi Polisi Keselamatan Siber KPK;	Pengurus ICT & Pentadbir Sistem
b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;	
c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga;	

d) Akses kepada aset ICT KPK perlu berlandaskan kepada perjanjian kontrak;

e) Memastikan semua syarat-syarat keselamatan dan prosedur dipatuhi dan dinyatakan dengan jelas kepada pihak ketiga;

Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai:

a) Polisi Keselamatan Siber KPK.
b) Tapisan Keselamatan.
c) Perakuan Akta Rahsia Rasmi 1972.
d) Hak Harta Intelek.

KAWALAN
03

PENGURUSAN ASET

KAWALAN 03
PENGURUSAN ASET

OBJEKTIF

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT KPK.

K03/01 TANGGUNGJAWAB TERHADAP ASET

K03/01/01 Inventori Aset ICT — **Tindakan**

Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing.

Perkara yang perlu dipatuhi adalah seperti berikut: — **Pegawai Aset ICT dan Semua**

a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dan dikemas kini;
b) Memastikan maklumat penyelenggaraan aset ICT direkod dan sentiasa dikemas kini;
c) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;
d) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di KPK;
e) Semua pergerakan dan peminjaman aset ICT direkod dan dipantau;
f) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan;
g) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya;
h) Peraturan bagi pengendalian pelupusan aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; dan
i) Penggunaan aset ICT KPK mestilah untuk tujuan tugas rasmi sahaja.

K03/01/02 Peminjaman dan Pemulangan Aset ICT	Tindakan

Peminjaman

Langkah-langkah perlu diambil termasuklah seperti berikut: **Pegawai Aset ICT**

a) mendapatkan kelulusan mengikut peraturan yang telah ditetapkan bagi membawa keluar peralatan bagi tujuan yang dibenarkan;
b) melindungi dan mengawal peralatan sepanjang masa;
c) merekodkan aktiviti peminjaman dan pemulangan peralatan; dan
d) menyemak peralatan ketika peminjaman dan pemulangan dilakukan.

Pemulangan

Memastikan semua aset ICT dikembalikan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan bagi pegawai yang ;

a) bertukar keluar;
b) bersara;
c) ditamatkan perkhidmatan; dan
d) diarahkan oleh Ketua Jabatan

Membatalkan atau menarik balik semua kebenaran capaian ke atas aset ICT mengikut peraturan yang ditetapkan.

K03/02 PENGELASAN DAN PENGENDALIAN MAKLUMAT

K03/02/01 Pengelasan Maklumat	Tindakan

Memastikan setiap maklumat diberikan tahap perlindungan yang bersesuaian. Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut Garis Panduan Keselamatan KPK. **BKPP, Semua SUB dan Ketua Unit**

Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan seperti berikut:

a) Rahsia Besar;
b) Rahsia;
c) Sulit; atau
d) Terhad.

K03/02/02 Pengendalian Maklumat	Tindakan
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut : a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan; e) Mematuhi *standard*, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g) Menjaga kerahsiaan langkah-langkah keselamatan siber dari diketahui umum.	**BKPP dan Semua**

K03/02/03 Pengurusan Rahsia Rasmi Dalam Persekitaran ICT	Tindakan
Jabatan yang menguruskan rahsia rasmi dalam persekitaran ICT hendaklah mematuhi tatacara pengurusan rahsia rasmi dan tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa.	**Semua**

K03/02/04 Pengelasan Rahsia Rasmi Dalam Persekitaran ICT	Tindakan
Rahsia rasmi perlu dikelaskan oleh Pegawai Pengelas yang dilantik di bawah Seksyen 2B Akta 88 berdasarkan kandungan, keutamaan dan tahap perlindungan keselamatan maklumat tersebut. Pengelasan	**BKPP dan Semua**

rahsia rasmi dalam persekitaran ICT hendaklah mengikut tatacara pengelasan yang ditetapkan oleh Kerajaan.

Sistem aplikasi yang menyimpan maklumat rahsia rasmi perlulah berupaya untuk memberikan tanda keselamatan pada setiap antara muka (*interface*) dan juga pada semua janaan dengan ciri-ciri keselamatan yang bersesuaian dengan peringkat keselamatan dan penilaian risiko.

K03/02/05 Pengelasan Semula Rahsia Rasmi Dalam Persekitaran ICT	**Tindakan**
Rahsia rasmi dalam persekitaran ICT perlulah dikaji dari semasa ke semasa bagi meringankan beban kepada sistem keselamatan secara keseluruhannya. KPK perlu mengambil tindakan untuk mengelaskan semula maklumat rahsia rasmi berdasarkan kepada peruntukan Seksyen 2C Akta 88 sekiranya maklumat berkenaan tidak lagi perlu menjadi rahsia rasmi.	**BKPP dan Semua**

K03/02/06 Pengendalian Maklumat Dalam Persekitaran ICT	**Tindakan**
Penyimpanan rahsia rasmi dalam persekitaran ICT hendaklah dilindungi secara fizikal dan logikal mengikut perkembangan teknologi. Pengguna kemudahan pengkomputeran bergerak (*mobile computing*) dalam memproses rahsia rasmi di luar pejabat hendaklah memastikan supaya ia sentiasa dilindungi daripada kehilangan dan kerosakan serta maklumat yang terkandung di dalamnya tidak dikrompomi. Semua hubungan komunikasi KPK seperti e-mel rasmi, *instant messaging*, *web conferencing*, perkongsian sumber, rangkaian tanpa wayar dan seumpamanya perlu dilindungi daripada capaian yang tidak dibenarkan. Maklumat rahsia rasmi hendaklah disediakan dalam bentuk fail kepilan (*attachment*) dan disulitkan (*encrypted*) sebelum dihantar kepada semua. E-mel yang mengandungi rahsia rasmi hendaklah berkeadaan disulitkan (*to be encrypted*) semasa dihantar dan disimpan serta dinyahsulitkan (*to be decrypted*) oleh penerima yang sah sahaja.	**Semua**

Penggunaan e-mel peribadi untuk urusan rahsia rasmi adalah dilarang sama sekali.

Penggunaan pengkomputeran awan (*cloud computing*) seperti perkongsian maklumat, pemprosesan data dan sebagainya bagi tujuan rahsia rasmi tidak dibenarkan sama sekali kecuali pengkomputeran awan yang dibangunkan dan dibenarkan oleh pihak Kerajaan dan tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa.

K03/02/07 Pemusnahan Rahsia Rasmi Dalam Persekitaran ICT	Tindakan
KPK hendaklah mendapatkan khidmat nasihat daripada Ketua Pengarah Keselamatan Kerajaan dan Ketua Pengarah Arkib Negara berhubung dengan pemusnahan maklumat rahsia rasmi sama ada mempunyai nilai arkib atau tidak, kelulusan Ketua Arkib Negara hendaklah diperoleh terlebih dahulu sebelum rahsia rasmi tersebut dimusnahkan.	BKPP

KAWALAN
04

KESELAMATAN SUMBER MANUSIA

KAWALAN 04
KESELAMATAN SUMBER MANUSIA

OBJEKTIF

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

K04/01 KESELAMATAN SUMBER MANUSIA

K04/01/01 Sebelum Perkhidmatan	Tindakan
Memastikan semua pengguna yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan KPK yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan b) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	PSM

K04/01/02 Semasa Perkhidmatan	Tindakan
Memastikan semua pekhidmat, kontraktor dan pihak ketiga mempunyai kesedaran terhadap ancaman keselamatan dan sedar akan tanggungjawab bagi memastikan segala dasar keselamatan dilaksanakan di dalam kerja yang dilakukan untuk menurunkan risiko akibat kesilapan manusia.	**Pengurus ICT**

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan KPK yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;
b) Memastikan pegawai dan kakitangan KPK serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh KPK;
c) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT KPK secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa;
d) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan KPK sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh KPK; dan
e) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan siber. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Pengurusan Sumber Manusia (PSM).

K04/01/03 Pertukaran atau Tamat Perkhidmatan	**Tindakan**

Memastikan pertukaran atau tamat perkhidmatan semua pengguna yang berkepentingan diuruskan dengan teratur.

Perkara yang perlu dipatuhi termasuk: **Pengurus ICT**

a) memastikan semua aset ICT dikembalikan kepada Kementerian mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan
b) membatalkan atau meminda semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut

KAWALAN
05

KESELAMATAN FIZIKAL DAN PERSEKITARAN

KAWALAN 05
KESELAMATAN FIZIKAL DAN PERSEKITARAN

OBJEKTIF

Melindungi premis dan aset ICT daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

K05/01 KESELAMATAN KAWASAN

K05/01/01 Keselamatan Kawasan Fizikal	Tindakan

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi.

Perkara-perkara yang perlu dipatuhi bergantung kepada hasil penilaian risiko termasuk yang berikut :

BKPP, ICTSO dan CIO

a) Kawasan keselamatan fizikal hendaklah dikenalpasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset;
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;
d) Menghadkan jalan keluar masuk;
e) Mengadakan kaunter kawalan;
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 kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk tersebut;
i) Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;
j) Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau bilau dan bencana;
k) Menyediakan garis panduan untuk kakitangan yang bekerja di kawasan terhad; dan
l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.

K05/01/02 Kawalan Masuk Fizikal	Tindakan
Kawalan Masuk Fizikal perlu dikenal pasti dan dilaksanakan ke atas kawasan yang menempatkan infrastruktur rangkaian dan komunikasi, fasiliti pemprosesan atau tempat penyimpanan maklumat terperingkat. Keselamatan fizikal termasuk keselamatan perimeter seperti pembinaan dinding, pagar kawalan dan menghadkan jalan keluar masuk ke kawasan berkenaan. Akses ke kawasan pejabat dan kawasan larangan perlu dikawal bagi memastikan hanya kakitangan atau pihak yang diberi tanggungjawab sahaja dibenarkan masuk.	BKPP dan Semua

K05/01/03 Kawasan Larangan ICT	Tindakan
Kawasan larangan ICT ditakrifkan sebagai kawasan di mana terdapat aset ICT kritikal yang boleh menjejaskan operasi dan keselamatan maklumat secara keseluruhan jika tidak dikawal. Kawasan larangan ICT di KPK ialah Bilik Server dan bilik/ruang yang terdapat peralatan ICT kritikal/kabel telekomunikasi (*MDF room/riser*). Akses kepada kawasan larangan hendaklah dikawal dan kebenaran hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	**BPM, BKPP dan Semua**

K05/01/04 Perlindungan Kawasan ICT Dari Ancaman Luar Dan Bencana Alam	Tindakan
Kawalan dan perlindungan keselamatan ke atas kawasan ICT perlu mengambilkira ancaman dari perbuatan manusia ataupun bencana alam seperti kebakaran, banjir, gempa bumi dan lain-lain.	**BPM, BKPP dan Semua**

K05/01/05 Kawalan Kawasan Penghantaran Barangan dan Loading Area	Tindakan
Kawasan penghantaran barangan dan *loading area* hendaklah dikawal dan perlu dipisahkan dari akses terus ke kawasan larangan	**BKPP**

K05/02 KESELAMATAN ASET ICT

K05/02/01 Peralatan dan Perkakasan ICT

Tindakan

Melindungi aset ICT dari kehilangan, kerosakan, kecurian aset serta gangguan kepada aset tersebut.

Semua aset ICT perlu dijaga dan dikawal dengan baik supaya ianya boleh digunakan sepanjang masa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

Semua

a) Pengguna hendaklah menyemak dan memastikan semua aset ICT di bawah kawalannya berfungsi dengan sempurna;
b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;
c) Pengguna dilarang sama sekali menambah, memanggil atau mengganti sebarang perkakasan ICT yang telah ditetapkan;
d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT;
e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;
f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;
g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;
h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;
i) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptible Power Supply* (UPS);
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 di dalam rak khas dan berkunci;
k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;
l) Peralatan ICT yang hendak dibawa keluar dari premis KPK perlulah mendapat kelulusan oleh pegawai yang diberikan kuasa dan direkodkan bagi tujuan pemantauan;

m) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera dan laporan polis hendaklah disertakan;
n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;
o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT dan Pegawai Aset KPK;
p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih;
q) Sebarang pelekat selain tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;
r) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;
s) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Sistem ICT;
t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya serta hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;
u) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "OFF" apabila meninggalkan pejabat;
v) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan
w) Memastikan suis ditutup bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.

K05/02/02 Clear Desk dan Clear Screen	**Tindakan**

Prosedur Clear Desk dan Clear Screen perlu dipatuhi supaya maklumat dalam apa jua bentuk media disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

a) menggunakan kemudahan *password screen saver* atau *log out* apabila meninggalkan komputer; **Semua**
b) menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan

c) memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat.

K05/02/03 Media Storan Digital	Tindakan

Media storan digital merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cekera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* dan media storan lain.

Media storan digital perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja;
c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;
d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet;
e) Akses dan pergerakan media storan hendaklah direkodkan;
f) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; — Semua
g) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data;
h) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan
i) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.

K05/02/04 Media Tandatangan Digital	Tindakan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

Semua

a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;
b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan
c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan selanjutnya.

K05/02/05 Media Perisian dan Aplikasi	Tindakan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

Semua

a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan KPK;
b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran CIO;
c) Keperluan lesen perisian daripada CD-ROM, *disk* atau media berkaitan bagi mengelakkan daripada berlakunya kecurian atau cetak rompak; dan
d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.

K05/02/06 Utiliti Sokongan	Tindakan

Semua utiliti sokongan perlu berada dalam keadaan terbaik dan mencukupi bagi menyokong sistem beroperasi. Utiliti sokongan ini termasuk bekalan elektrik, air, pendingin hawa, generator, alat komunikasi dan lain-lain.

Semua

K05/02/07 Penyelenggaraan Perkakasan	Tindakan

Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti adalah terkawal.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Semua perkakasan perlu diselenggara mengikut spesifikasi yang telah ditetapkan oleh pengeluar;
b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;

c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau setelah tamat tempoh jaminan; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f) Semua penyelenggaraan mestilah mendapat kebenaran daripada pegawai yang diberikan tanggungjawab menjaganya.	**Semua**

K05/02/08 Aset ICT di Luar Premis	**Tindakan**

Aset ICT seperti storan penyimpanan maklumat, komputer peribadi, *computer tablet*, telefon mudah alih, *smart card*, dokumen atau lain-lain perkakasan yang dibawa keluar daripada premis KPK perlu dilindungi dari risiko keselamatan seperti kecurian, kerosakan dan lain-lain.

Antara perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Aset yang hendak dibawa keluar dari premis perlu mendapat kebenaran; b) Pegawai adalah bertanggungjawab sepenuhnya ke atas aset yang dibawa keluar; c) Aset perlu dilindungi dan dikawal sepanjang masa; d) Maklumat pada aset hendaklah sentiasa dilindungi dengan katakunci; dan e) Penyimpanan atau penempatan aset mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	**Semua**

K05/02/09 Pelupusan dan Guna Semula Perkakasan	**Tindakan**

Pelupusan melibatkan semua aset ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh KPK dan ditempatkan di KPK.

Aset ICT yang akan dilupuskan atau diguna semula, terutama yang mengandungi maklumat terperingkat atau perisian yang dilesenkan, perlu diuruskan dengan teratur dan selamat mengikut prosedur pelupusan semasa atau guna semula peralatan yang telah ditetapkan. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan KPK.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Semua kandungan perkakasan khususnya maklumat terperingkat hendaklah dihapuskan terlebih dahulu sebelum pelupusan atau diguna semula;
b) Pelupusan Aset ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;
c) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran; **BKPP dan Semua**
d) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan;
e) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;
f) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;
g) Peralatan yang hendak dilupuskan mestilah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;
h) Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Inventori; dan
i) Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut:
    i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya;
    ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana Bahagian KPK;

iii. Memindah keluar dari KPK mana-mana peralatan ICT yang hendak dilupuskan;
iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab BKPP; dan
v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti *disket* atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.

K05/02/10 Perkakasan Tanpa Penyeliaan (*Unattended Equipment*)	**Tindakan**
Pengguna perlu memastikan mana-mana perkakasan yang ditinggalkan tanpa penyeliaan mematuhi ciri-ciri keselamatan seperti mempunyai kata laluan dan sebagainya. Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.	**Semua**

K05/02/11 Penyelenggaraan	**Tindakan**
Peralatan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut: a) mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang di selenggara; b) memastikan perkakasan hanya diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c) menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan d) memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	**Pentadbir Sistem, Pegawai Aset ICT**

K05/03 KESELAMATAN PERSEKITARAN

K05/03/01 Kawalan Persekitaran	**Tindakan**

Melindungi aset ICT KPK dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa atau mengubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pegawai Keselamatan Kerajaan dan ICTSO.

Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi :

BKPP dan Semua

a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik pencetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;
b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegahan kebakaran dan pintu kecemasan;
c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;
d) Bahan mudah terbakar hendaklah disimpan di luar kawasan bersesuaian dan berjauhan dari aset ICT;
e) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer;
f) Semua cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT;
g) Semua peralatan perlindungan hendaklah diselenggara dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan
h) Akses kepada saluran *riser* hendaklah sentiasa dikunci.

K05/03/02 Bekalan Kuasa — **Tindakan**

Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Semua peralatan ICT kritikal hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; **BKPP dan BPM**
b) Peralatan sokongan seperti *Uninterruptible Power Supply* (UPS) dan/atau penjana (*generator*) hendaklah digunakan bagi perkhidmatan kritikal seperti di bilik server supaya sentiasa mendapat bekalan kuasa berterusan; dan
c) Semua peralatan sokongan bekalan kuasa hendaklah diperiksa dan diuji secara berjadual.

K05/03/03 Kabel Rangkaian	**Tindakan**

Kabel rangkaian hendaklah dilindungi kerana ia boleh menyebabkan maklumat terdedah.

Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:

a) Menggunakan kabel rangkaian yang mengikuti spesifikasi yang telah ditetapkan; **BKPP dan BPM**
b) Melindungi kabel rangkaian daripada kerosakan yang disengajakan atau tidak disengajakan;
c) Melindungi laluan pemasangan kabel rangkaian sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan
d) Semua kabel rangkaian perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel rangkaian daripada kerosakan dan pintasan maklumat.

K05/03/04 Prosedur Kecemasan Persekitaran	**Tindakan**

Prosedur kecemasan persekitaran seperti kebakaran, banjir, bencana alam dan lain-lain yang melibatkan persekitaran kawasan ICT terjejas hendaklah di kaji dari semasa ke semasa.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan KPK; dan
b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut aras.

BKPP

K05/03/05 Mekanisme Pelaporan Insiden Bukan ICT	**Tindakan**
Semua pengguna yang terlibat haruslah melaporkan dan merekodkan sebarang kejadian atau kerosakan peralatan bukan ICT kepada pihak pentadbiran bahagian.	**Semua**

K05/03/06 Mekanisme Kawalan Peralatan Sewaan/Ujicuba *(Proof Of Concept)*	**Tindakan**
Penerimaan: a) Peralatan yang diterima bebas daripada virus, *backdoor, worm* dan perkara-perkara yang boleh memberi ancaman kepada perkhidmatan ICT Kementerian.	**Pentadbir Sistem**

Penyelenggaraan:

a) Capaian melalui rangkaian luar KPK adalah tidak dibenarkan; dan
b) Aktiviti penyelenggaraan adalah di bawah pengawasan pegawai KPK.

Pemulangan:

a) Maklumat yang tersimpan dalam storan perlu dihapuskan secara kekal (*secured delete*); dan
b) Memastikan semua maklumat jabatan tidak tertinggal pada peralatan.

K05/04 KESELAMATAN DOKUMEN

K05/04/01 Dokumen	Tindakan
Melindungi maklumat KPK dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut Prosedur Arahan Keselamatan; d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa sepertimana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan e) Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	**Semua**

KAWALAN
06

KESELAMATAN OPERASI

KAWALAN 06
KESELAMATAN OPERASI

OBJEKTIF

Memastikan pengurusan operasi ICT berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

K06/01 PENGURUSAN PROSEDUR OPERASI DAN TANGGUNGJAWAB

K06/01/01 Pengendalian Prosedur Operasi ICT — Tindakan

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

Pentadbir Sistem

a) Semua prosedur pengurusan operasi yang diwujudkan, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal;
b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan
c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan, diberikan nombor versi pindaan dan diluluskan oleh Pengurus ICT.

K06/01/02 Kawalan Perubahan — Tindakan

Perubahan yang melibatkan perkakasan rangkaian dan komunikasi, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah dikemukakan oleh pemilik sistem atau pentadbir rangkaian dan komunikasi serta mendapat kebenaran daripada pegawai yang diberi kuasa.

Sebarang perubahan komponen sistem ICT hendaklah mematuhi keperluan yang ditetapkan.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

a) Pengubahsuaian yang melibatkan perkakasan rangkaian dan komunikasi, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; — **Pentadbir Sistem**
b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;
c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan
d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.

K06/01/03 Pengasingan Tugas dan Tanggungjawab	Tindakan

Tugas dan tanggungjawab setiap pegawai perlu ditetapkan dengan jelas bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; — **Pengurus ICT dan Pentadbir Sistem**
b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan
c) Perkakasan yang digunakan bagi membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

K06/02 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PIHAK KETIGA

K06/02/01 Perkhidmatan	Tindakan

Memastikan penyampaian perkhidmatan pihak ketiga mematuhi tahap keselamatan yang ditetapkan selaras dengan perjanjian perkhidmatan.

Pihak ketiga perlu mematuhi terma dan syarat-syarat berkaitan kawalan keselamatan yang telah ditetapkan dalam perjanjian — **Pengurus ICT dan Semua**

Perkara-perkara yang mesti dipatuhi adalah seperti berikut :

a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga;
b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan
c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.

K06/02/02 Pemantauan Perkhidmatan Pihak Ketiga	**Tindakan**
Perkhidmatan, laporan dan rekod pihak ketiga perlu dipantau, disemak dan diaudit.	**Pengurus ICT**

K06/03 PERANCANGAN DAN PENERIMAAN SISTEM

K06/03/01 Perancangan Kapasiti	**Tindakan**
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada	**Pentadbir Sistem**

perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

K06/03/02 Penerimaan Sistem	Tindakan
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. Sijil penerimaan sistem hanya akan dikeluarkan setelah segala ujian penerimaan yang ditetapkan berjaya dilaksanakan sepenuhnya.	Pentadbir Sistem

K06/04 KAWALAN TERHADAP PERISIAN BERBAHAYA

K06/04/01 Perlindungan Dari Perisian Berbahaya	Tindakan
Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *trojan* dan sebagainya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa; c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d) Mengemaskini antivirus dengan *pattern* antivirus yang terkini; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini	Pentadbir Sistem Semua

bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;

h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan
i) Memberi amaran mengenai ancaman keselamatan siber seperti serangan virus.

K06/04/02 Kawalan terhadap kod berbahaya (*Malicious Code)*	Tindakan
Perisian atau sistem yang digunakan mesti bebas daripada kod berbahaya (*malicious code)*.	Pentadbir Sistem

K06/04/03 Kawalan terhadap *Mobile Code*	Tindakan
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Pentadbir Sistem

K06/05 HOUSEKEEPING (BACKUP)

K06/05/01 *Backup*	Tindakan
Melindungi integriti maklumat agar boleh diakses pada bila-bila masa. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah mengikut prosedur yang telah ditetapkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan;	Pengurus ICT dan Semua Pentadbir Sistem

d) Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan
e) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.

K06/06 PENGENDALIAN MEDIA

K06/06/01 Penghantaran dan Pemindahan	Tindakan
Melindungi media mudah alih dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan perkhidmatan. Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu dan perlu mematuhi prosedur yang ditetapkan.	Pengguna

K06/06/02 Prosedur Pengendalian Dan Pelupusan Media	Tindakan
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut: a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat ; b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e) Menyimpan semua media di tempat yang selamat; dan f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	Pengguna

K06/06/03 Keselamatan Sistem Dokumentasi	Tindakan
Sistem dokumentasi perlu disimpan dengan selamat dan dilindungi daripada capaian yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	Pengguna

K06/06/04 Maklumat Capaian Umum	Tindakan
Maklumat yang dipaparkan perlu mempunyai tahap integriti yang tinggi dan dilindungi dari pindaan yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti yang berikut : a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; b) Memastikan sistem yang boleh diakses oleh pengguna diuji terlebih dahulu; dan c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Semua

K06/07 PERKHIDMATAN E-DAGANG (*ELECTRONIC COMMERCE SERVICES*)

K06/07/01 E-Dagang	Tindakan

Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.

Perkhidmatan E-Dagang melalui kemudahan Internet adalah dibenarkan dengan kawalan bagi menjamin keselamatan maklumat.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan;

b) Maklumat yang terlibat dalam transaksi dalam talian (*online*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan

c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.

Pengurus ICT, Pemilik Sistem dan Semua

K06/07/02 Transaksi atas talian	Tindakan
Maklumat yang terlibat dalam transaksi atas talian (*online*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian dan pendedahan yang tidak dibenarkan.	**Pemilik Sistem dan Pentadbir Sistem**

K06/08 PEMANTAUAN

K06/08/01 Pengauditan dan Forensik ICT	Tindakan
Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	

Pentadbir Sistem mestilah bertanggungjawab mengesan, merekod dan menganalisis perkara-perkara berikut :

ICTSO dan Pentadbir Sistem

a) Sebarang percubaan pencerobohan kepada sistem ICT KPK;

b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), spam, pemalsuan (*forgery phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*);

c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesuatu sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;

d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti Kerajaan;

e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;

f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwitdth*) rangkaian;

g) Aktiviti penyalahgunaan akaun e-mel; dan

h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.

K06/08/02 Jejak Audit (*Audit Trail*) **Tindakan**

Sistem kritikal mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara

kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara.

Jejak audit hendaklah mengandungi maklumat-maklumat berikut:

a) Rekod setiap aktiviti transaksi;

Pentadbir Sistem

b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;

c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan

d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.

Jejak audit hendaklah disimpan untuk tempoh masa yang ditetapkan oleh pihak pengurusan atau peraturan semasa.

Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.

K06/08/03 Sistem Log	**Tindakan**

Bagi memastikan aktiviti sistem kritikal dipantau, Pentadbir Sistem ICT perlu melaksanakan perkara-perkara berikut :

a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; **Pentadbir Sistem**

b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan

c) Sekiranya wujud aktiviti-aktiviti yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.

K06/08/04 Pemantauan Log	Tindakan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; **Pentadbir Sistem**

b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala;

c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;

d) Aktiviti pentadbiran dan operator sistem perlu direkodkan;

e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan

f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam KPK atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.

K06/08/05 Perlindungan Log	Tindakan

Maklumat dan fasiliti log perlu dilindungi daripada capaian yang tidak dibenarkan.	**Pentadbir Sistem**

K06/08/06 Log untuk Pentadbir Sistem	**Tindakan**
Segala aktiviti pentadbir dan operator sistem perlu direkod.	**Pentadbir Sistem**

K06/08/07 Log Kerosakan	**Tindakan**
Segala kerosakan perlu direkod, dianalisa dan diambil tindakan.	**Pentadbir Sistem**

K06/08/08 Penyeragaman Waktu	**Tindakan**
Semua sistem ICT KPK perlu mempunyai waktu yang seragam dengan *Network Time Protokol* (NTP) KPK atau waktu yang dinyatakan oleh SIRIM.	**Pentadbir Sistem**

KAWALAN 07
KESELAMATAN KOMUNIKASI

OBJEKTIF

Memastikan maklumat dan infrastruktur rangkaian dilindungi dan mempunyai ciri-ciri keselamatan siber yang bersesuaian.

K07/01 PENGURUSAN KESELAMATAN RANGKAIAN

K07/01/01 Kawalan Infrastruktur Rangkaian — Tindakan

Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; — **Pengurus ICT, ICTSO dan Pentadbir Rangkaian**

b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;

c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;

d) Semua peralatan mestilah melalui proses *Factory Acceptance Check* (*FAC*) semasa pemasangan dan konfigurasi;

e) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Sistem ICT;

f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan KPK;

g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;

h) Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat KPK;

i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;

j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan KPK adalah tidak dibenarkan;

k) Semua pengguna hanya dibenarkan menggunakan rangkaian KPK sahaja dan penggunaan modem adalah dilarang sama sekali;

l) Semua peralatan yang hendak disambung kepada rangkaian perlu bebas daripada virus dan mempunyai *antivirus* yang sah;

m) Capaian kepada rangkaian perlu dilaksanakan mengikut kategori yang telah ditetapkan iaitu Intranet, Internet dan DMZ;

n) Peralatan persendirian adalah dilarang untuk capaian kepada rangkaian Intranet KPK;

o) Sistem yang terdapat di dalam rangkaian Intranet tidak dibenarkan dicapai dari Internet;

p) Pihak ketiga adalah tidak dibenarkan untuk mencapai rangkaian Intranet kecuali untuk kerja-kerja pembangunan atau penyelenggaraan sistem dengan kebenaran pemilik sistem; dan

q) Capaian kepada *wireless* hendaklah dikawal mengikut kategori pengguna.

K07/02 PENGURUSAN PERTUKARAN MAKLUMAT

K07/02/01 Pertukaran Maklumat	Tindakan
Memastikan keselamatan pertukaran maklumat dan perisian antara KPK dan agensi luar terjamin. Pertukaran maklumat mesti mendapat kelulusan dari pihak pengurusan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara KPK dengan agensi luar; c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari KPK; dan d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua

K07/02/02 Pengurusan Mel Elektronik (E-Mel)	Tindakan
Penggunaan e-mel di KPK hendaklah dipantau secara berterusan dan hendaklah mematuhi etika dan peraturan yang ditetapkan oleh KPK. Pengguna e-mel perlu mematuhi perkara-perkara berikut: a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh KPK sahaja boleh digunakan semasa membuat urusan rasmi;	Semua

b) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;

c) Hanya warga KPK atau pengguna yang dibenarkan sahaja boleh dipertimbangkan untuk mendapat kemudahan e-mel rasmi Kementerian;

d) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

e) Pegawai Tadbir Bahagian perlu memaklumkan sebarang status pengguna (bertukar jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke KPK) di bahagian masing-masing bagi tujuan pengemaskinian e-mel yang terlibat;

f) Pengguna perlu memastikan saiz e-mel yang dihantar tidak melebihi saiz yang ditetapkan oleh penerima;

g) Pengguna tidak dibenarkan menghantar lampiran (*attachment*) melebihi had yang ditetapkan;

h) Pengguna bertanggungjawab membuat salinan atau *backup* e-mel;

i) Pengguna hendaklah menyemak dan menentukan tarikh dan masa sistem komputer adalah sentiasa tepat;

j) Pengguna perlu memastikan semua e-mel dibaca dan diambil tindakan segera;

k) Pengguna perlu memastikan *mailbox* mempunyai ruangan storan yang cukup terutama untuk transaksi di hujung minggu atau cuti; dan

l) Pengguna bertanggungjawab untuk mengemaskini *mailbox* masing-masing.

K07/02/03 Business Information System	Tindakan
Maklumat yang terlibat dalam perkongsian data di antara sistem aplikasi perlu dilindungi.	Pentadbir Laman Web dan Semua

KAWALAN
08

KAWALAN CAPAIAN

KAWALAN 08
KAWALAN CAPAIAN

OBJEKTIF

Memastikan capaian kepada maklumat adalah berdasarkan kepada keperluan organisasi dan keselamatan maklumat.

K08/01 KAWALAN CAPAIAN

K08/01/01 Keperluan Kawalan Capaian — Tindakan

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; — **Pentadbir Sistem**

b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;

c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan

d) Kawalan ke atas kemudahan pemprosesan maklumat.

K08/02 PENGURUSAN CAPAIAN PENGGUNA

K08/02/01 Pendaftaran Akaun Pengguna — Tindakan

Mengawal capaian pengguna ke atas aset ICT KPK.

Pendaftaran, pengemaskinian dan penamatan akaun penguna mestilah dilaksanakan mengikut prosedur yang ditetapkan. Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan.

Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi:

a) Akaun pengguna hanya diwujudkan setelah mendapat pengesahan Bahagian Pengurusan Sumber Manusia dan pengguna telah mengesahkan memahami Polisi Keselamatan Siber (PKS); **Semua**

b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;

c) Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja;

d) Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;

e) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan KPK. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;

f) Penggunaan akaun milik individu lain adalah dilarang;

g) Akaun pengguna tidak boleh dikongsi; dan

h) Akaun pengguna boleh dibeku atau ditamatkan apabila menerima arahan daripada Bahagian Pengurusan Sumber Manusia atas sebab-sebab berikut:

   i. Pengguna bercuti panjang dalam tempoh waktu melebihi tiga (3) minggu;
   ii. Bertukar bidang tugas kerja;
   iii. Bertukar ke agensi lain;

iv. Bersara;
v. Bagi menjalankan siasatan; atau
vi. Ditamatkan perkhidmatan.

K08/02/02 Hak Capaian *(Privilege)*	Tindakan
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas dan juga atas prinsip perlu mengetahui (*need-to-know-basis*)	**Pemilik Sistem dan Pentadbir Sistem ICT**

K08/02/03 Semakan Hak Capaian Pengguna	Tindakan
Pemilik sistem perlu menyemak semula hak capaian pengguna dari semasa ke semasa	**Pentadbir Sistem ICT**

K08/02/04 Pengurusan Kata Laluan Pengguna	Tindakan
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta garis panduan yang ditetapkan oleh KPK. Penggunaan *default administrator* dan *guest* adalah tidak dibenarkan sama sekali.	**Semua**

K08/03 TANGGUNGJAWAB PENGGUNA

K08/03/01 Penggunaan Akaun dan Kata Laluan	Tindakan
Menghalang capaian yang tidak dibenarkan terhadap maklumat dan fasiliti pemprosesan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;	**Semua**

c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khas;

d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun;

e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;

f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;

g) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula;

h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;

i) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan;

j) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan

k) Mengelakkan penggunaan semula kata laluan yang baru digunakan sebelum ini.

K08/03/02 Perkakasan Tanpa Penyeliaan	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a) Komputer yang *idle* dalam tempoh 15 minit perlu di *lock screen*;	**Semua**

b) Semua peralatan komputer perlu di *log off* setelah tugasan selesai; dan

c) Kawalan yang bersesuaian perlu dilaksanakan bagi peralatan tanpa pengawasan.

K08/03/03 Clear Desk dan Clear Screen	Tindakan

Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada di atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya

a) Pengguna perlu *lock screen* apabila meninggalkan komputer pada bila-bila masa; **Semua**

b) Semua fail atau dokumen terperingkat perlu disimpan di tempat yang berkunci apabila meninggalkan meja kerja;

c) Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan; dan

d) Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

i. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer;

ii. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan

iii. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.

K08/03/04 Penggunaan Komputer/*Notebook*	Tindakan

Penggunaan aset komputer KPK termasuk desktop dan *notebook* perlu dikawal supaya tiada pencerobohan, penyalahgunaan, kecurian, kehilangan dan pengubahsuaian kepada maklumat.

Semua pengguna komputer KPK perlu mematuhi perkara berikut:

Semua

a) Semua komputer KPK hendaklah digunakan untuk tugas rasmi sahaja;

b) Pengguna bertanggungjawab memastikan bahawa komputer perlu sentiasa mempunyai *antivirus* yang aktif dan terkini;

c) Semua komputer perlu didaftar pemiliknya dan pemilik berkenaan adalah bertanggungjawab menjaga keselamatan komputer tersebut sehingga komputer tersebut dilupuskan;

d) Setiausaha Bahagian adalah bertanggungjawab terhadap komputer gunasama, dan setiap pergerakan komputer tersebut perlu direkodkan;

e) Komputer (*notebook*) yang dibekalkan kepada pegawai yang layak, dibenarkan untuk dibawa pulang atau dibawa ke mana-mana dan pegawai adalah bertanggungjawab menjaga keselamatan aset berkenaan sepanjang masa;

f) Pentadbir Sistem berhak untuk menyiasat kandungan komputer apabila menerima arahan daripada CIO atau ICTSO;

g) Komputer milik KPK saja yang dibenarkan untuk mencapai maklumat-maklumat yang terdapat di dalam Intranet;

h) Komputer milik KPK perlu menggunakan domain KPK bagi mencapai ke rangkaian dan sistem-sistem KPK;

i) Komputer milik KPK adalah dilarang digunakan oleh pihak ketiga tanpa kawalan dan pengawasan pegawai KPK; dan

j) Pegawai perlu melaporkan dengan segera sekiranya berlaku kehilangan komputer atau *notebook* kepada KPK dengan menyertakan salinan laporan Polis.

K08/04 KAWALAN CAPAIAN RANGKAIAN

K08/04/01 Capaian Rangkaian	Tindakan
Menghalang capaian yang tidak sah dan tanpa kebenaran ke atas perkhidmatan Rangkaian (wayar dan tanpa wayar) KPK. Penggunaan perkhidmatan rangkaian diberikan kepada pengguna berasaskan kepada tugas dan skop kerja. Semua sistem/aplikasi atau pengguna perlu mematuhi kawalan capaian perkhidmatan rangkaian yang ditetapkan seperti berikut: a) Semua capaian akan berasaskan kepada tiga (3) *zone* rangkaian iaitu Intranet, *Demilitarized Zone* (DMZ) dan Internet ; b) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian KPK, rangkaian agensi lain dan rangkaian awam; c) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunanya; d) Menghalang mana-mana pengguna awam memasuki ke rangkaian intranet tanpa pengawasan; e) Kontraktor atau pihak ketiga adalah dilarang membawa keluar peralatan yang digunakan untuk mencapai rangkaian intranet kecuali telah mendapat pengesahan pemilik sistem; dan f) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	**Pentadbir Rangkaian, Pengurus ICT dan Semua**

K08/04/02 Capaian Internet	Tindakan

Capaian melalui Internet (Rangkaian Awam) kepada rangkaian dan maklumat KPK hendaklah dikawal bagi memastikan tiada berlaku kecurian, pencerobohan, kerosakan dan pengubahsuaian.

Pengguna KPK yang berdaftar adalah dibenarkan untuk mencapai Internet dengan kawalan berasaskan tugas-tugas rasmi dan skop kerja.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Capaian ke Intranet KPK menggunakan Internet atau rangkaian awam adalah tidak dibenarkan;

b) Penggunaan Internet di KPK hendaklah dipantau secara berterusan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja seperti yang terdapat di dalam tatacara penggunaan Internet;

c) Penggunaan *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;

Pentadbir Rangkaian, Pengurus ICT dan Semua

d) Semua aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu disekat bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan;

e) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja, CIO berhak menentukan penggunaan yang dibenarkan atau sebaliknya;

f) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh ICTSO atau CIO;

g) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Setiausaha Bahagian sebelum dimuat naik ke Internet;

h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah Hak Cipta Terpelihara;

i) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh KPK;

j) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board* atau sebagainya. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan;

k) Penggunaan *modem/broadband* pada mana-mana peralatan atau aset yang berada atau bersambung dengan rangkaian KPK adalah tidak dibenarkan sama sekali; dan

l) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:

i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan

ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.

K08/04/03 Peralatan Dalam Rangkaian	**Tindakan**

Bagi memastikan bahawa peralatan yang disambungkan kepada Rangkaian KPK tidak menjejaskan keselamatan maklumat dan capaian, maka perkara-perkara berikut hendaklah dipatuhi:

a) Setiap peralatan yang hendak disambung kepada rangkaian KPK perlu didaftarkan;

b) Semua peralatan perlu disahkan bebas daripada virus dan perisian *antivirus* hendaklah dipasang dan masih aktif sepanjang masa;

c) Hanya peralatan yang telah berdaftar dibenarkan untuk sambungan (*join*) kepada rangkaian;

d) Setiap peralatan yang hendak disambung ke rangkaian perlu menggunakan protokol TCP/IP dan akan menggunakan IP *address* dan *domain name* yang ditetapkan oleh pentadbir rangkaian; dan

e) Semua konfigurasi peralatan dalam rangkaian selepas *switches* adalah menjadi tanggungjawab pengguna.

Pentadbir Rangkaian

K08/04/04 Capaian Ke *Port* Untuk Tujuan Diagnostik	Tindakan

Bagi memastikan bahawa *port* rangkaian tidak dicapai tanpa pengawasan, perkara berikut perlu dipatuhi oleh semua pengguna:

a) Semua *port* yang tak digunakan perlu *disable*;

b) Capaian fizikal dan logikal ke atas *port* untuk tujuan diagnostik perlu mendapat kebenaran pegawai yang diberikan kuasa;

c) Capaian oleh pegawai KPK hanya dibenarkan berasaskan kepada tugas dan skop kerja; dan

d) Capaian oleh pihak ketiga perlu mendapat kelulusan dari pegawai yang diberikan kuasa.

Pentadbir Rangkaian

K08/04/05 Pengasingan Dalam Rangkaian	Tindakan

Rangkaian KPK perlu dibuat pengasingan menggunakan VLAN, Zon (Intranet, DMZ, Internet) dan VPN mengikut jenis perkhidmatan, pengguna, sensitiviti maklumat dan sistem.

Pentadbir Rangkaian

K08/04/06 Penghalaan *(Routing)* Rangkaian	Tindakan
Penghalaan (*routing*) perlu dikawal supaya ianya tidak disalah guna dengan memastikan perkara berikut:	
a) Konfigurasi (*routing*) perlu disemak dan disahkan sebelum dilaksanakan;	**Pentadbir Rangkaian**
b) Semakan *routing table* perlu dibuat dari semasa ke semasa; dan	
c) Penghalaan (*routing*) di dalam sistem rangkaian perlu dilaksanakan dengan betul dan terkawal.	

K08/05 KAWALAN CAPAIAN SISTEM PENGOPERASIAN

K08/05/01 Capaian Sistem Pengoperasian	Tindakan
Menghalang capaian yang tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu diaktifkan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi:	
a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan	**Pentadbir Sistem**
b) Merekodkan capaian yang berjaya dan gagal.	
Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut:	
a) Mengesahkan pengguna yang dibenarkan; dan	
b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*.	

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin;

b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;

c) Menghadkan dan mengawal penggunaan program; dan

d) Menghadkan tempoh sambungan ke aplikasi berisiko tinggi.

K08/05/02 Secure Log-on	Tindakan
Log-on ke atas sistem pengoperasian perlu melalui satu kaedah yang selamat bagi mengurangkan akses yang tidak dibenarkan.	Pentadbir Sistem

K08/05/03 Pengenalan dan Pengesahan pengguna	Tindakan
Capaian masuk sistem perlu mempunyai kaedah bagi mengenal dan mengesahkan pengguna adalah sah.	Pentadbir Sistem

K08/05/04 Penggunaan Sistem Utiliti	Tindakan
Penggunaan sistem utiliti perlulah dikawal dan dihadkan kepada pegawai yang dibenarkan saja.	Pentadbir Sistem

K08/05/05 Session Time-Out	Tindakan
Sesi yang tidak aktif perlu ditamatkan mengikut tempoh masa yang ditetapkan.	

	Pentadbir Sistem dan Pentadbir Rangkaian
K08/05/06 Had Masa Capaian	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	
a) Had masa capaian kepada maklumat dan sistem aplikasi hendaklah berasaskan kepada keperluan dan fungsi pengguna; dan b) Masa capaian bagi aplikasi berisiko tinggi perlu dihadkan semasa waktu pejabat sahaja.	**Pentadbir Sistem**
K08/05/07 Token / Sijil Digital	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	
a) penggunaan token Kerajaan Elektronik (Token EG) atau sijil digital hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; b) token hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c) perkongsian penggunaan token adalah tidak dibenarkan sama sekali; dan d) sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada pengeluar token.	**Pengguna**

K08/06 KAWALAN CAPAIAN APLIKASI DAN MAKLUMAT

K08/06/01 Capaian Aplikasi dan Maklumat — Tindakan

Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.

Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi:

Semua

a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang diberikan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;

b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log);

c) Menghadkan capaian sistem dan aplikasi kepada tiga (5) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;

d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan

e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja dan di dalam zon yang ditetapkan.

K08/06/02 Larangan Capaian Maklumat — Tindakan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

Semua

a) Capaian kepada maklumat dan sistem aplikasi hendaklah berasaskan kepada keperluan dan fungsi pengguna;

b) Capaian kepada maklumat yang tidak rasmi , berunsur lucah, iklan dan yang menjejaskan prestasi kerja; dan

c) Capaian kepada maklumat dan sistem aplikasi perlu dinyatakan dengan jelas kepada pengguna.

K08/06/03 Pengasingan Sistem Kritikal	Tindakan
Pengasingan sistem kritikal perlu dilaksana dengan menggunakan VLAN/ VPN dan zon rangkaian (intranet, DMZ, Internet).	Pentadbir Sistem

K08/07 PERALATAN MUDAH ALIH DAN KERJA JARAK JAUH

K08/07/01 Peralatan Mudah Alih	Tindakan
Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh. Perkara yang perlu dipatuhi adalah seperti berikut: a) Peralatan mudah alih yang dikhaskan untuk pegawai yang berkelayakan dibenarkan dibawa keluar bagi melaksanakan tugas-tugas rasmi; b) Peralatan mudah alih gunasama perlu direkod dan mendapat kelulusan pegawai yang bertanggungjawab apabila hendak dibawa keluar dari pejabat; c) Semua peralatan mudah alih hendaklah dilindungi dan dikawal dengan selamat; dan d) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua

K08/07/02 Kemudahan Kerja Jarak Jauh	Tindakan
Kerja jarak jauh hanya boleh dilaksanakan setelah mendapat kelulusan pegawai yang diberi kuasa dan pemilik sistem yang berkaitan. Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian yang tidak sah serta salah guna kemudahan.	Semua

K08/08 KAWALAN BRING YOUR OWN DEVICE (BYOD)

K08/08/01 Bring Your Own Device (BYOD)	Tindakan
BYOD merupakan peralatan mudah alih persendirian seperti telefon pintar, tablet dan laptop yang digunakan oleh pengguna yang melaksanakan tugas rasmi melalui sambungan rangkaian Jabatan. Pengguna yang menggunakan kemudahan wifi jabatan atau data line persendirian untuk akses kepada Internet tertakluk kepada PKS KPK. Sebagai garis panduan, pengguna bertanggungjawab memastikan langkah-langkah keselamatan perlindungan berkaitan penggunaan BYOD seperti berikut : a) mengelak risiko kebocoran maklumat rasmi; b) mengelakkan ancaman risiko keselamatan ICT; c) memastikan produktiviti pengguna tidak terjejas dalam menjalankan urusan rasmi jabatan; dan d) meningkatkan integriti data. Bagi mengawal dan memantau pelaksanaan BYOD, mekanisme kawalan diwujudkan seperti berikut:	Semua

a) mendaftarkan penggunaan peralatan mudah alih yang digunakan melalui AD;

b) mengaktifkan fungsi keselamatan kata laluan bagi mengelakkan akses yang tidak dibenarkan; dan

c) melaporkan kehilangan peralatan mudah alih kepada ICTSO.

Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada penggunaan BYOD.

KAWALAN
09

KAWALAN KRIPTOGRAFI

KAWALAN 09
KESEAMATAN KRIPTOGRAFI

OBJEKTIF

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi mengikut keperluan.

K09/01 KAWALAN KRIPTOGRAFI

K09/01/01 Enkripsi	Tindakan
Proses enkripsi (*encryption*) perlu dilaksanakan bagi melindungi kerahsiaan maklumat kritikal atau sensitif berdasarkan keperluan, penilaian risiko dan selaras dengan Akta-akta KPK.	Semua

K09/01/02 Tandatangan Digital	Tindakan
Penggunaan tandatangan digital (sekiranya berkaitan) adalah dimestikan kepada semua pengguna khususnya yang berurusan dengan transaksi maklumat kritikal atau sensitif atau maklumat rahsia rasmi secara elektronik.	Semua

K09/01/03 Pengurusan Kunci Kriptografi	Tindakan
Pengurusan kunci kriptografi yang dilaksanakan ke atas maklumat kritikal atau sensitif hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut. Kriptografi turut merangkumi kaedah-kaedah seperti berikut: a) Kesemua pelaksanaan sistem hendaklah menggunakan ID atau kata laluan dan dibuat enkripsi; b) Penggunaan PKI (*Public Key Infrastructure*) yang selamat yang dibekalkan oleh Kerajaan.	Semua

KAWALAN
10

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

KAWALAN 10
PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

K10/01 KESELAMATAN DALAM MEMBANGUNKAN SISTEM & APLIKASI MUDAH ALIH

Objektif

Memastikan sistem dan aplikasi mudah alih yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan siber yang bersesuaian.

K10/01/01 Keperluan Keselamatan Sistem Maklumat	Tindakan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem dan aplikasi mudah alih hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketetapan maklumat; — **Pentadbir Sistem, Pemilik Sistem dan ICTSO**

b) Ujian keselamatan hendaklah dijalankan ke atas sistem dan aplikasi mudah alih baru dibangunkan, ditambah baik atau dinaik taraf yang merangkumi perkara berikut:

   i. menyemak pengesahan dan integriti data input yang dimasukkan;

   ii. memastikan sistem pemprosesan berfungsi dengan betul dan sempurna; dan

   iii. memastikan data yang diproses menghasilkan output yang tepat;

c) Sistem dan aplikasi mudah alih perlu mengandungi semakan pengesahan (*vadilation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan.

K10/01/02 Analisa Dan Spesifikasi Keperluan Keselamatan	Tindakan
Spesifikasi reka bentuk perlu mengandungi keperluan keselamatan sistem maklumat. Sekiranya sesuatu produk *off-the-shelf* diperolehi, pembekal perlu dimaklumkan berkenaan keperluan keselamatan.	Pentadbir Sistem

K10/02 KEBOLEHPERCAYAAN PEMPROSESAN DALAM SISTEM & APLIKASI MUDAH ALIH

Objektif

Untuk mengelak kesalahan, kecacatan, kerugian, pengubahsuaian yang tidak dibenarkan, penyalahgunaan maklumat atau kehilangan kepercayaan terhadap sistem dan aplikasi mudah alih.

K10/02/01 Pengesahan Data Input	Tindakan
Data yang dimasukkan ke dalam sistem dan aplikasi mudah alih perlu disahkan untuk memastikan data adalah tepat dan betul.	Pentadbir Sistem

K10/02/02 Kawalan Bagi Pemprosesan Dalaman	Tindakan
Satu prosedur semakan perlu diadakan di dalam sistem dan aplikasi mudah alih bagi mengesan sebarang kerosakan maklumat yang terhasil daripada kesilapan dan kecacatan pemprosesan ataupun kesalahan yang disengajakan. Senarai semak yang bersesuaian perlu disediakan, aktiviti-aktiviti hendaklah didokumenkan dan hasil keputusan perlu disimpan dengan selamat.	Pentadbir Sistem

K10/02/03 Integriti Maklumat	Tindakan
Satu penilaian terhadap risiko keselamatan perlu dijalankan untuk menentukan keperluan integriti maklumat dan bagi mengenal pasti kaedah yang paling bersesuaian untuk dilaksanakan.	Pemilik Sistem dan Pentadbir Sistem

K10/02/04 Pengesahan Data *Output*	Tindakan

Data yang dikeluarkan daripada sistem dan aplikasi mudah alih perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat. **Pemilik Sistem**

K10/03 KESELAMATAN FAIL SISTEM

Objektif

Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.

K10/03/01 Kawalan Perisian (*Operational Software*) — Tindakan

Kawalan perubahan kepada perisian perlu dilaksanakan bagi mengurangkan risiko kerosakan pada perisian. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

a) Proses pengemaskinian perisian hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang diberi tanggungjawab dan mengikut prosedur yang telah ditetapkan; **Pentadbir Sistem**

b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh digunakan selepas diuji dan diluluskan;

c) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan;

d) Mengawal capaian ke atas kod atau cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan

e) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal.

Semua sistem konfigurasi perlu didaftar dan didokumenkan.

K10/03/02 Kawalan Data Pengujian Sistem	Tindakan
Data pengujian sistem perlu dipilih dengan teliti, dilindungi dan terkawal. Penggunaan data sebenar (*operational data*) yang melibatkan data personel atau data sensitif pada persekitaran pengujian perlu dielakkan. Jika data personel atau data sensitif digunakan untuk tujuan pengujian, kandungan sensitif perlu ditapis atau diubahsuai sebelum digunakan.	**Pemilik Sistem**

K10/03/03 Kawalan Capaian kepada Kod Sumber (*Source Code*)	Tindakan
Kawalan capaian kepada kod sumber atau atur cara program perlu dilaksanakan bagi mengelakkan kecurian, pengubahsuaian dan penghapusan tanpa kebenaran. Kod sumber bagi semua aplikasi dan perisian adalah menjadi hak milik KPK.	**Pentadbir Sistem**

K10/04 KESELAMATAN DALAM PROSES PEMBANGUNAN & PROSES SOKONGAN

Objektif

Menjaga dan menjamin keselamatan sistem perisian aplikasi dan maklumat.

K10/04/01 Kawalan Perubahan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perubahan dan pengubahsuaian ke atas sistem perisian aplikasi dan maklumat perlu dikawal, diuji, direkodkan dan disahkan melalui prosedur yang ditetapkan sebelum diguna pakai; b) Pengujian terhadap perubahan dan pengubahsuaian ke atas sistem perisian aplikasi dan maklumat hendaklah dilaksanakan dalam persekitaran yang berasingan daripada produksi dan pembangunan;	**Pentadbir Sistem dan Pemilik Sistem**

c) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi.

d) Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor;

e) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;

f) Akses kepada kod sumber aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan

g) Menghalang sebarang peluang untuk membocorkan maklumat.

K10/04/02 Keperluan Kajian Teknikal Terhadap Aplikasi Selepas Perubahan Sistem Pengoperasian	**Tindakan**
Semua aplikasi perlu dikaji dan diuji apabila berlaku perubahan sistem pengoperasian bagi memastikan tiada sebarang kesan buruk yang merugikan kepada operasi dan keselamatan organisasi.	**Pentadbir Sistem**

K10/04/03 Pembangunan Perisian Secara *Outsource*	**Tindakan**
Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. Kod sumber bagi semua aplikasi dan perisian adalah menjadi hak milik KPK.	**Pemilik Sistem dan Pentadbir Sistem**

K10/05 PENGURUSAN KELEMAHAN TEKNIKAL

Objektif

🎯 Mengurangkan risiko akibat daripada eksploitasi kelemahan teknikal.

K10/05/01 Kawalan Kelemahan Teknikal	Tindakan
Kelemahan teknikal terhadap sistem maklumat perlu dilapor dan dibuat penilaian dengan segera untuk tindakan pembetulan.	Pemilik Sistem dan Pentadbir Sistem

K10/06 KAWALAN TEKNIKAL KETERDEDAHAN (VULNERABILITY)

Objektif

Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.

K10/06/01 Kawalan dari Ancaman Teknikal	Tindakan
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan.	
Perkara yang perlu dipatuhi adalah seperti berikut :	
a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan;	Pentadbir Sistem
b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan	
c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	

KAWALAN
II

HUBUNGAN PEMBEKAL

KAWALAN 11
HUBUNGAN PEMBEKAL

OBJEKTIF

Memastikan aset ICT KPK yang boleh dicapai oleh pembekal dilindungi.

K11/01 KAWALAN HUBUNGAN PEMBEKAL

K11/01/01 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal — **Tindakan**

Semua pembekal adalah tertakluk kepada Dasar Keselamatan Kerajaan yang sedang berkuat kuasa.

Perkara–perkara yang perlu dipatuhi adalah seperti berikut: — **Pengurus ICT, Pembekal**

a) pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas;
b) pengurusan pembekal adalah tertakluk kepada peraturan yang sedang berkuat kuasa;
c) pengawalan dan pemantauan akses pembekal; dan
d) keperluan minimum keselamatan maklumat bagi setiap pembekal seperti keperluan perundangan atau pekeliling berkaitan hendaklah dinyatakan dalam perjanjian.

K11/01/02 Pengurusan Penyampaian Perkhidmatan Pembekal — **Tindakan**

Bertujuan untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dengan penyampaian perkhidmatan adalah sama seperti perjanjian pembekal.

KPK hendaklah sentiasa memantau, mengkaji semula dan mengaudit penyampaian perkhidmatan pembekal. Perkara-perkara berikut hendaklah dipatuhi: — **Pengurus ICT, Pentadbir Sistem**

a) pemantauan tahap prestasi perkhidmatan bagi mengesahkan pembekal mematuhi perjanjian perkhidmatan; dan

b) laporan perkhidmatan yang dihasilkan oleh pembekal dan status kemajuan yang dikemukakan kepada KPK hendaklah dipantau.

Semua perubahan perkhidmatan pembekal hendaklah dilaksanakan secara teratur dan mengikut peraturan-peraturan semasa.

Perkara-perkara yang perlu diambil kira adalah seperti berikut:

c) perubahan dalam perjanjian dengan pembekal;
d) perubahan yang dilakukan oleh KPK bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan
e) perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.

KAWALAN
12

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

KAWALAN 12

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

K12/01 MEKANISME PELAPORAN INSIDEN KESELAMATAN SIBER

Objektif

Memastikan insiden keselamatan siber dan kelemahan dilapor dan disalurkan dengan cepat dan berkesan bagi meminimumkan proses pembaikan dan mengurangkan kesan insiden keselamatan siber.

K12/01/01 Mekanisme Pelaporan	Tindakan
Insiden keselamatan siber bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar Polisi Keselamatan Siber (PKS) sama ada yang ditetapkan secara tersurat atau tersirat.	
Insiden keselamatan siber seperti berikut hendaklah dilaporkan kepada ICTSO dan CSIRT KPK dengan kadar segera: a) Maklumat didapati hilang, didedahkan oleh pihak-pihak yang diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c) Kata laluan atau mekanisme kawalan akses dicuri, didedahkan atau disyaki hilang; d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e) Berlaku percubaan pencerobohan, penyelewengan dan insiden-insiden yang tidak dijangka yang boleh menjejaskan keselamatan siber.	Semua

Prosedur pelaporan insiden keselamatan siber di KPK hendaklah berdasarkan:

a) Surat Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan Pengendalian Insiden Keselamatan Siber Sektor Awam.

K12/01/02 Pelaporan Kelemahan Keselamatan	Tindakan
Pengguna sistem dikehendaki melaporkan sebarang kelemahan sistem dengan segera bagi mengelak insiden keselamatan siber.	Semua

K12/02 PENGURUSAN MAKLUMAT INSIDEN KESELAMATAN SIBER

Objektif

Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan siber

K12/02/01 Maklumat Insiden Keselamatan Siber	Tindakan
Maklumat mengenai insiden keselamatan siber yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden di masa akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada KPK. Bahan-bahan bukti berkaitan insiden keselamatan siber hendaklah disimpan dan diselenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:	Pengurus ICT dan ICTSO

a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti;

b) Menyalin bahan bukti dan merekodkan semua maklumat dan aktiviti penyalinan;

c) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan;

d) Menyediakan tindakan pemulihan segera; dan

e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.

K12/02/02 Pembelajaran Dari Insiden Kelemahan Maklumat	Tindakan
Mewujudkan mekanisma bagi menentukan semua insiden keselamatan maklumat direkod untuk dianalisa dan dipantau.	ICTSO dan Pentadbir Sistem

K12/02/03 Pengumpulan Bukti	Tindakan
Bukti-bukti insiden keselamatan maklumat perlu dikumpul dan dikekalkan untuk tindakan perundangan.	ICTSO dan Pentadbir Sistem

KAWALAN
13

KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

KAWALAN 13
PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

K13/01 DASAR KESINAMBUNGAN PERKHIDMATAN

Objektif

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

K13/01/01 Pelan Kesinambungan Perkhidmatan	Tindakan
Pelan Kesinambungan Perkhidmatan (*Business Continuity Plan (BCP)*) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh pihak pengurusan KPK atau mana-mana jawatankuasa yang ditubuhkan. Perkara-perkara berikut perlu diber perhatian: a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan siber; c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; d) Mendokumentasikan proses dan prosedur yang telah dipersetujui; e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;	**PSA dan BKPP**

f) Membuat *backup*; dan

g) Menguji dan mengemas kini pelan sekurang-kurangnya sekali (1) setahun.

Pelan Kesinambungan Perkhidmatan mempunyai tiga komponen utama iaitu:-

a) Pelan Pemulihan Bencana;

b) Pelan Tindak Balas Kecemasan; dan

c) Pelan Komunikasi Krisis.

DAN hendaklah mengandungi perkara-perkara berikut:

a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;

b) Senarai personel KPK dan vendor berserta nombor yang boleh dihubungi (faks, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel yang tidak dapat hadir untuk menangani insiden;

c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;

d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan

e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan yang mana perlu.

Salinan BCP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. BCP hendaklah diuji sekurang-kurangnya sekali (1) setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah

dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi objektif pembangunan.

Ujian BCP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. KPK hendaklah memastikan salinan BCP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

KAWALAN
14

PEMATUHAN

KAWALAN 14
PEMATUHAN

K14/01 PEMATUHAN DAN KEPERLUAN PERUNDANGAN

Objektif

Meningkatkan tahap keselamatan siber bagi mengelak dari pelanggaran kepada Polisi Keselamatan Siber (PKS) KPK.

K14/01/01 Pematuhan Dasar	Tindakan
Setiap pengguna di KPK hendaklah membaca, memahami dan mematuhi Polisi Keselamatan Siber (PKS) KPK dan undang-undang atau peraturan-peraturan lain yang berkuat kuasa. Semua aset ICT di KPK termasuk maklumat yang disimpan di dalamnya adalah hak milik KPK. KSU atau pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna bagi mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT KPK selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber KPK.	**Semua**

K14/01/02 Pematuhan Dasar dan Keperluan Teknikal	Tindakan
ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar dan keperluan teknikal.	**ICTSO**

K14/01/03 Pematuhan Keperluan Audit	Tindakan
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	**Semua**

K14/01/04 Keperluan Perundangan	Tindakan
Semua pengguna aset ICT KPK perlu mematuhi segala keperluan perundangan, akta atau peraturan-peraturan lain yang berkaitan yang terpakai oleh KPK. Senarai Perundangan dan Peraturan adalah seperti di **LAMPIRAN 2**.	**Semua**

K14/01/05 Pelanggaran Dasar	Tindakan
Pelanggaran Polisi Keselamatan Siber KPK boleh dikenakan tindakan tatatertib menurut polisi yang diluluskan seperti tindakan undang-undang dan tatatertib di bawah Akta Rahsia Rasmi 1972 dan Perintah-perintah Am Bab "D" – Peraturan-peraturan Pegawai Awam (kelakuan Dan Tatatertib).	**Semua**

LAMPIRAN

LAMPIRAN 1

SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER (PKS) KEMENTERIAN PERLADANGAN DAN KOMODITI (KPK)

Nama (Huruf Besar) :
No. Kad Pengenalan :
Jawatan :
Bahagian/Unit :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

i. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber KPK.
ii. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : _____

Tarikh : _____

Pengesahan Pegawai Keselamatan ICT (ICTSO)

_____
Pegawai Keselamatan ICT (ICTSO)
b.p. Ketua Setiausaha KPK
Tarikh : _____

LAMPIRAN 2

SENARAI PERUNDANGAN DAN PERATURAN

1. Arahan Keselamatan;
2. Akta Tandatangan Digital 1997;
3. Akta Rahsia Rasmi 1972;
4. Akta Jenayah Komputer 1997;
5. Akta Hak Cipta (Pindaan) Tahun 1997;
6. Akta Komunikasi dan Multimedia 1998;
7. Arahan Keselamatan;
8. Akta Tandatangan Digital 1997;
9. Akta Rahsia Rasmi 1972;
10. Akta Jenayah Komputer 1997;
11. Akta Hak Cipta (Pindaan) Tahun 1997;
12. Akta Komunikasi dan Multimedia 1998;
13. Akta 709 – Akta Perlindungan Data Peribadi 2010;
14. Akta 658 – Akta Perdagangan Elektronik 2006;
15. Akta 629 – Akta Arkib Negara 2003;
16. Akta 606 – Akta Cakera Optik 2000;
17. Akta 298 – Kawasan Larangan Tempat Larangan 1959;
18. Akta 56 – Akta Keterangan 1950;
19. Arahan Keselamatan;
20. Arahan Perbendaharaan;
21. Arahan Teknologi Maklumat 2007;
22. Arahan 20 (Semakan Semula) – Dasar dan Mekanisme Pengurusan Bencana Negara;
23. Arahan 24 – Dasar dan Mekanisme Pengurusan Krisis Siber Negara;
24. Dasar Pengurusan Rekod dan Arkib Elektronik;
25. Garis Panduan Penerapan Etika Penggunaan Media Sosial Dalam Sektor Awam (MAMPU);
26. Garis Panduan Perolehan ICT Kerajaan Kementerian Kewangan Malaysia. Cabutan Pekeliling Perbendaharaan Malaysia PK 2.2/2013;
27. Garis Panduan IT Outsourcing Agensi-agensi Sektor Awam 14/2006;
28. Garis Panduan Pengurusan Rekod;
29. Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi;
30. Guideline to Determine Information Security Professionals Requirement for the CNII Agencies/Organisation;
31. National Cyber Security Policy (NCSP);
32. Panduan Pelaksanaan ISMS Sektor Awam;

33. Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 bertajuk "Pengurusan Laman Web Agensi Sektor Awam);

34. Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 bertajuk "Panduan Pengurusan Pejabat Bertarikh 30 April 2007";

35. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;

36. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;

37. Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam;

38. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;

39. Pekeliling Transformasi Pentadbiran Awam Bilangan 3 Tahun 2007 Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan;

40. Pekeliling Am Bilangan 1 Tahun 2015- Pelaksanaan Data Terbuka Sektor Awam;

41. Pekeliling Perbendaharaan Malaysia PK2/2013- Kaedah Perolehan Kerajaan;

42. Perintah-perintah Am;

43. PK 3.2 – Manual Perolehan Perkhidmatan Perunding Edisi 2011 (Pindaan Kedua);

44. Pekeliling Perbendaharaan AM 2 Tahun 2018 : Tatacara Pengurusan Aset Alih Kerajaan;

45. Rancangan Malaysia Ke-12;

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

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

48. Surat Arahan Ketua Pengarah MAMPU Pelaksanaan dan Penggunaan Aplikasi Digital Document Management System (DDMS) Sektor Awam yang bertarikh 26 Januari 2015;

49. Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat yang bertarikh 24 November 2010;

50. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010;

51. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

52. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) di

Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;

53. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;

54. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;

55. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;

56. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);

57. Surat Pekeliling Perbendaharaan Bil. 2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

58. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;

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

60. Surat Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2015 bertajuk "Panduan Pelaksanaan Program Turun Padang Sektor Awam";

61. Perintah-Perintah Am;

62. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;

63. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.

64. Surat Pekeliling Perbendaharaan – Garis Panduan Mengenai Pengurusan Perolehan *Information Telecommunication Technology* ICT Kerajaan SPP 3/2013;

65. Surat Pekeliling Am Bilangan 2/1987 – Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987);

66. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSA) versi 1.0 April 2016;

67. Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bil.1/2021 – Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam;

68. Pekeliling Perbendaharaan (PP)/ Pekeliling Perolehan (PK) 2.6 – Perkhidmatan Pengkomputeran Awan (Cloud) Sektor Awam;

69. Surat Pekeliling Am Bil.2 Tahun 2021 - Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam

70. Strategik Keselamatan Siber Malaysia 2020 – 2024 (NACSA)

KEMENTERIAN PERLADANGAN
DAN KOMODITI

KEMENTERIAN PERLADANGAN DAN KOMODITI
No. 15, Level 5-13, Persiaran Perdana, Presint 2,
Pusat Pentadbiran Kerajaan Persekutuan
62654 Wilayah Persekutuan Putrajaya
https://www.mpic.gov.my/

ISBN 978-967-19545-9-1
9 7 8 9 6 7 1 9 5 4 5 9 1