



POLISI KESELAMATAN SIBER

Jabatan Perkhidmatan Awam
VERSI

1.1





POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

i dari vi

KANDUNGAN

BIL.	PERKARA	M/S
1.	SEJARAH POLISI KESELAMATAN SIBER JPA	1
2.	Pengenalan	2
3.	Objektif	2
4.	Pernyataan Polisi	3
5.	SKOP	5
6.	Prinsip-Prinsip	7
7.	Penilaian Risiko Keselamatan ICT	9
8.	Pelan Pengurusan Keselamatan Maklumat	10
9.	Kawalan-Kawalan	

KAWALAN 01 – POLISI KESELAMATAN MAKLUMAT

Objektif	13
K01/01 Pelaksanaan Dasar	13
K01/02 Penyebaran Dasar	13
K01/03 Penyelenggaraan Dasar	13
K01/04 Pematuhan Dasar	14

KAWALAN 02 - ORGANISASI KESELAMATAN MAKLUMAT

Objektif	15
K02/01 Tadbir Urus Keselamatan Maklumat	15
K02/01/01 Ketua Pengarah Perkhidmatan Awam (KPPA)	15
K02/01/02 Ketua Pegawai Maklumat (CIO)	15
K02/01/03 Pegawai Keselamatan ICT (ICTSO)	16
K02/01/04 Pengurus ICT	17
K02/01/05 Pentadbir Sistem	19
Pentadbir Rangkaian Dan Keselamatan	19
Pentadbir Pangkalan Data	20
Pentadbir Portal (Web Master)	21
Pentadbir Pusat Data	22
Pentadbir Sistem Aplikasi	23
Pentadbir E-mel	24
Pentadbir Media Sosial JPA	25
Pegawai Aset ICT	25
K02/01/06 Pengguna	28
K02/01/07 Jawatankuasa Pemandu ICT (JPICIT) JPA	30
K02/01/08 Jawatankuasa Keselamatan ICT (JKICT) JPA	32
K02/01/09 Pasukan Tindak Balas Insiden Keselamatan ICT (JPACERT)	34
K02/01/10 Jawatankuasa Pelan Pemulihan Bencana (JKDRP) JPA	35



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

ii dari vi

K02/02 Pihak Luaran	36
K02/02/01 Keperluan Keselamatan Dalam Perkhidmatan ICT	36

KAWALAN 03 – KESELAMATAN SUMBER MANUSIA

Objektif	39
K03/01 Sebelum Perkhidmatan	39
K03/02 Semasa Perkhidmatan	39
K03/03 Bertukar Atau Tamat Perkhidmatan	40

KAWALAN 04 - PENGURUSAN ASET

Objektif	42
K04/01 Akauntabiliti Aset ICT	42
K04/02 Peminjaman dan Pemulangan Aset ICT	43
K04/03 Pengelasan Maklumat	44
K04/04 Pengendalian Maklumat	44
K04/05 Pengelasan dan Pengendalian Data Terbuka	45
K04/06 Pengendalian Media	46
K04/06/01 Media Storan	46

KAWALAN 05 – KAWALAN CAPAIAN

Objektif	48
K05/01 Kawalan Capaian	48
K05/02 Pengurusan Capaian Pengguna	48
K05/02/01 Pendaftaran Pengguna	48
K05/02/02 Hak Capaian	49
K05/02/03 Pengurusan Kata Laluan	49
K05/03 Capaian Sistem Pengoperasian	51
K05/03/01 Capaian Sistem Pengoperasian	51
K05/03/02 Token/ Sijil Digital	53
K05/04 Capaian Aplikasi dan Maklumat	53
K05/05 Capaian Jarak Jauh	54
K05/06 Kawalan Capaian Rangkaian	55
K05/06/01 Capaian Rangkaian	55
K05/06/02 Capaian Internet	56
K05/07 Peralatan Mudah Alih	57
K05/08 Bring Your Own Device (BYOD)	57

KAWALAN 06 – KAWALAN KRIPTOGRAFI

Objektif	59
K06/01 Kriptografi	59
K06/01/01 Enkripsi	59
K06/01/02 Public Key Infrastructure (PKI)	59
K06/01/03 Tandatangan Digital	60



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

iii dari vi

KAWALAN 07 – KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif	61
K07/01 Keselamatan Kawasan	61
K07/01/01 Kawasan Larangan Lokasi ICT	61
K07/01/02 Kawalan Masuk Fizikal	62
K07/02 Keselamatan Peralatan	63
K07/02/01 Peralatan ICT	63
K07/02/02 <i>Clear Desk</i> dan <i>Clear Screen</i>	65
K07/02/03 Media Tandatangan Digital	65
K07/02/04 Perisian dan Aplikasi	66
K07/02/05 Peralatan Tanpa Penyeliaan (Unattended Equipment)	67
K07/02/06 Peralatan di Luar Premis	67
K07/02/07 Pelupusan	68
K07/02/08 Penyelenggaraan	69
K07/03 Kawalan Persekitaran	69
K07/03/01 Kawalan Persekitaran	69
K07/03/02 Kabel Rangkaian	70
K07/03/03 Bekalan Kuasa	71
K07/03/04 Prosedur Kecemasan	71
K07/03/05 Mekanisme Pelaporan Insiden Bukan ICT	72
K07/03/06 Mekanisme Kawalan Peralatan Sewaan/Ujicuba (Proof Of Concept)	72
K07/04 Keselamatan Sistem Dokumentasi	73

KAWALAN 08 – KESELAMATAN OPERASI

Objektif	74
K08/01 Prosedur Operasi	74
K08/01/01 Pengendalian Dokumen Prosedur Operasi	74
K08/01/02 Pengurusan Perubahan	74
K08/01/03 Pengasingan Tugas dan Tanggungjawab	75
K08/02 Perancangan dan Penerimaan Sistem	76
K08/02/01 Perancangan Kapasiti	76
K08/02/02 Penerimaan Sistem	76
K08/03 Perlindungan dari Perisian Berbahaya	76
K08/03/01 Perlindungan dari Perisian Berbahaya	76
K08/03/02 Perlindungan dari <i>Mobile Code</i>	78
K08/04 Housekeeping	78
K08/04/01 <i>Backup</i>	78
K08/05 Pengurusan Media	79
K08/05/01 Media Storan Mudah Alih	79
K08/05/02 Prosedur Pengendalian Media	79
K08/06 Paparan Maklumat Umum	80
K08/07 Pemantauan	80
K08/07/01 Pemantauan	80
K08/07/02 Pengauditan dan Forensik ICT	81
K08/07/03 Jejak Audit	82



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

iv dari vi

K08/07/04 Sistem Log	83
K08/07/05 Penyeragaman Waktu (Time Synchronisation)	84
K08/07/06 Kawalan Pengoperasian Perisian	84
K08/07/07 Pengurusan Kerentanan Teknikal	85

KAWALAN 09 – KESELAMATAN KOMUNIKASI

Objektif	87
K09/01 Pengurusan Rangkaian	87
K09/02 Pengurusan Penghantaran dan Penerimaan Maklumat	88
K09/03 Pengurusan Mel Elektronik (E-mel)	89

KAWALAN 10 – PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Objektif	91
K10/01 Kawalan Prosesan Aplikasi	91
K10/01/01 Pengesahan Data <i>Input</i>	91
K10/01/02 Kawalan Prosesan	91
K10/01/03 Pengesahan Data <i>Output</i>	92
K10/02 Keselamatan Fail Sistem	92
K10/03 Keselamatan Dalam Proses Pembangunan Dan Sokongan	93
K10/03/01 Peraturan Keselamatan Dalam Pembangunan Sistem	93
K10/03/02 Prosedur Perubahan	93
K10/03/03 Semakan Teknikal Aplikasi Selepas Perubahan Platform	93
K10/03/04 Kawalan Terhadap Perubahan Kepada Perisian	93
K10/03/05 Prinsip Kejuruteraan Sistem Yang Selamat	94
K10/03/06 Persekitaran Pembangunan Sistem Yang Selamat	94
K10/03/07 Pembangunan Sistem Secara Luar (Outsource)	94
K10/03/08 Ujian Keselamatan Sistem	95
K10/03/09 Pembocoran Maklumat	95
K10/04 Data Ujian	95
K10/05 Kawalan Terhadap Keterdedahan Teknikal	95
K10/06 Perkhidmatan E-Dagang	96
K10/07 Pembangunan Aplikasi Mudah Alih	96
K10/07/01 Prosedur Integrasi Pembangunan Aplikasi Mudah Alih	96



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

v dari vi

KAWALAN 11 – HUBUNGAN PEMBEKAL

Objektif	97
K11/01 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal	97
K11/02 Pengurusan Penyampaian Perkhidmatan Pembekal	97

KAWALAN 12 – RISIKO DAN PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

Objektif	99
K12/01 Mekanisme Pelaporan Insiden Keselamatan ICT	99
K12/02 Prosedur Pengurusan dan Pengendalian Insiden Keselamatan ICT	101

KAWALAN 13 – KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Objektif	102
K13/01 Pengurusan Kesenambungan Perkhidmatan	102
K13/01/01 Pelan Pemulihan Bencana	104
K13/02 Lewahan (Redundancy)	105

KAWALAN 14 – PEMATUHAN

Objektif	106
K14/01 Pematuhan Dasar	106
K14/02 Pematuhan kepada Dasar, Peraturan dan Penilaian Teknikal Keselamatan	107
K14/03 Pematuhan Keperluan Audit	107
K14/04 Pelanggaran Perundangan	108

10.	GLOSARI	109
-----	---------	-----

11. SENARAI LAMPIRAN

Lampiran 1	Surat Akuan Pematuhan Polisi Keselamatan Siber JPA	119
Lampiran 2	Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT JPA	120
Lampiran 3	Permohonan Kebenaran Untuk Menggunakan Kemudahan Internet Peribadi Bagi Tujuan Sambungan Ke Internet	122



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

vi dari vi

Lampiran 4 *Official Secrets Act* (OSA)

124

Lampiran 5 Senarai Perundangan dan Peraturan

126



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

1 dari 128

SEJARAH POLISI KESELAMATAN SIBER JPA

VERSI	KELULUSAN	TARIKH KUATKUASA
1.0	JPICT	18 DISEMBER 2020
1.1	JPICT	16 NOVEMBER 2021



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

2 dari 128

PENGENALAN

Polisi Keselamatan Siber Jabatan Perkhidmatan Awam (JPA) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi semasa menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Polisi ini juga menerangkan kepada pengguna mengenai tanggungjawab dan peranan pengguna dalam melindungi aset ICT JPA. Polisi Keselamatan Siber (PKS) JPA disediakan berpandu kepada piawaian antarabangsa iaitu ISO/IEC 27001:2013.

OBJEKTIF

Objektif utama PKS adalah seperti berikut:

1. memastikan kelancaran operasi jabatan yang berlandaskan ICT dengan mencegah serta meminimumkan risiko kerosakan atau kemusnahan aset ICT jabatan;
2. melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan daripada segi kerahsiaan, integriti, tidak boleh disangkal, ketersediaan dan kesahihan;
3. meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan aset ICT;
4. meningkatkan tahap kesedaran keselamatan ICT kepada para kakitangan, pengguna dan pihak luaran;



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

3 dari 128

PERNYATAAN POLISI

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

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

1. melindungi maklumat rasmi JPA dari capaian tanpa kuasa yang sah;
2. menjamin setiap maklumat adalah tepat, lengkap dan terkini;
3. memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
4. memastikan akses hanya kepada pengguna yang sah dan penerimaan maklumat daripada sumber yang boleh dipercayai.

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

1. Kerahsiaan – maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan akses tanpa kebenaran.
2. Integriti – data dan maklumat hendaklah tepat, lengkap dan terkini. Ia hanya boleh diubah dengan cara yang dibenarkan sahaja.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

4 dari 128

3. Tidak boleh disangkal – punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal.
4. Kesahihan – data dan maklumat hendaklah dijamin kesahihannya.
5. Ketersediaan – data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain itu, analisa tahap risiko aset ICT dikenalpasti, seterusnya mengambil tindakan untuk merancang dan mengawal risiko berkenaan.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

5 dari 128

SKOP

Sistem ICT JPA terdiri daripada organisasi, manusia, perisian, peralatan, telekomunikasi, kemudahan ICT, data dan maklumat. JPA telah menetapkan keperluan-keperluan asas keselamatan seperti berikut:

1. data dan maklumat termasuk *hardcopy* dan *softcopy* hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan dengan cara yang boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.
2. semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan melindungi kepentingan JPA.

PKS JPA merangkumi perlindungan ke atas semua bentuk maklumat ICT kerajaan yang dimasukkan, diwujudkan, dimusnah, disimpan, dijana, dicetak, diakses, diedar dan yang dibuat salinan. Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

1. Data dan maklumat
Semua data dan maklumat elektronik dan bercetak yang disimpan atau digunakan di pelbagai media termasuk prosedur, manual pengguna, sistem dokumentasi, rekod, pangkalan data dan lain-lain;
2. Peralatan ICT
Semua peralatan komputer seperti, komputer peribadi, komputer riba pencetak, media storan, server, firewall, peralatan multimedia & komunikasi, dan alat sokongan yang lain;



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

6 dari 128

3. Perisian

Semua jenis perisian yang digunakan untuk mengendali, memproses, menyimpan dan menghantar data atau maklumat. Ini termasuklah sistem aplikasi seperti HRMIS, eSILA, EPSA dan perisian sistem seperti Windows, LINUX dan perisian utiliti, perisian komunikasi, sistem pengurusan pangkalan data, kod sumber dan lain-lain;

4. Perkhidmatan

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

Contoh:

- i. perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
- ii. sistem halangan akses seperti sistem kad akses; dan
- iii. perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegahan kebakaran dan lain-lain.

5. Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian bagi mencapai misi dan objektif;

6. Persekitaran Fizikal

Persekitaran fizikal yang merujuk kepada lokasi fizikal yang menempatkan perkara 1-5 di atas.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

7 dari 128

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada PKS JPA adalah seperti berikut:

1. Akses Atas Dasar Perlu Mengetahui

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

2. Hak Akses Minimum

Hak akses kepada pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas diperlukan untuk membolehkan pengguna mencipta, menyimpan, mengemas kini, mengubah dan menghapuskan sesuatu data atau maklumat.

3. 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. Bagi menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesahkan bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

4. Pengasingan

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



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

8 dari 128

5. Pengauditan

Tujuan aktiviti ini ialah untuk mengenal pasti insiden keselamatan aset ICT atau keadaan yang mengancam keselamatan aset ICT. Dengan itu, semua log yang berkaitan dengan aset ICT perlu disimpan bagi tujuan jejak audit.

6. Pematuhan

PKS JPA hendaklah dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

7. Pemulihan

Pemulihan sistem amat perlu untuk memastikan ketersediaan dan kebolehcapaian bagi meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui proses penduaan (backup) dan mewujudkan Pelan Pemulihan Bencana (DRP) di bawah Pengurusan Kesenambungan Perkhidmatan (PKP).

8. Saling Bergantung

Setiap prinsip adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan, dapat menjamin keselamatan yang maksimum.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

9 dari 128

PENILAIAN RISIKO KESELAMATAN ICT

JPA hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat daripada ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu JPA 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.

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

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat JPA termasuklah aplikasi, perisian, peralatan, pelayan, rangkaian, pangkalan data, sumber manusia, proses, dan 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 sokongan lain.

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

JPA perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

1. mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
2. menerima atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan atasan;
3. mengelak atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak atau mencegah berlakunya risiko; dan
4. memindahkan risiko kepada pihak luaran yang berkepentingan.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

10 dari 128

PELAN PENGURUSAN KESELAMATAN MAKLUMAT

Setiap projek di JPA hendaklah menyediakan Pelan Pengurusan Keselamatan Maklumat. Pelan ini mengandungi maklumat terperinci yang menyatakan keutamaan aplikasi, kawalan capaian dan keperluan-keperluan khusus yang lain.

Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), Polisi Keselamatan Siber JPA dan surat pekeliling/arahan terkini untuk menangani isu-isu operasi projek.

Pelan ini hendaklah mengenal pasti perlindungan data-dalam-penggunaan, data-dalam-pergerakan, data dalam-simpanan dan menghalang ketirisan data.

Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

1. Peranti Pengkomputeran Peribadi

Peranti Pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, telefon pintar, tablet dan peranti storan.

2. Peranti Rangkaian

- a. Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti *switch*, *router*, *firewall*, peranti VPN dan kabel.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

11 dari 128

- b. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat

3. Aplikasi

- a. Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi, sistem operasi.
- b. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

4. Pelayan

- a. Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat.
- b. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

5. Persekitaran Fizikal

- a. Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan aset ICT.
- b. JPA hendaklah merujuk ke Pejabat Ketua Pegawai Keselamatan Kerajaan untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.
- c. Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip *defence-in-depth*.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

12 dari 128

- d. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.



POLISI KESELAMATAN MAKLUMAT

KAWALAN

Polisi Keselamatan Siber JPA Versi 1.1

01



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

13 dari 128

Kawalan 01: Polisi Keselamatan Maklumat

Objektif

PKS JPA ini diwujudkan untuk melindungi aset ICT bagi memastikan kelancaran operasi jabatan 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, ketersediaan dan kesahihan.

K01/01 Pelaksanaan Dasar

Pelaksanaan dasar ini akan dikuatkuasakan oleh Ketua Pengarah Perkhidmatan Awam (KPPA), dan dibantu oleh Jawatankuasa Pemandu ICT JPA (JPIC) yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan semua Pengarah Bahagian.

KPPA

K01/02 Penyebaran Dasar

Dasar ini perlu disebar kepada semua pengguna.

ICTSO

K01/03 Penyelenggaraan Dasar

PKS JPA adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan PKS JPA:

- mengenal pasti dan menentukan perubahan yang diperlukan;
- mengemukakan cadangan untuk pertimbangan Jawatankuasa Keselamatan ICT (JKICT);

ICTSO, JKICT



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

14 dari 128

- c. memaklumkan cadangan pindaan untuk perakuan oleh JKICT dan kelulusan JPICT;
- d. memaklumkan pindaan yang telah diluluskan oleh JPICT kepada semua pengguna; dan
- e. menyemak semula dokumen sekurang-kurangnya setahun sekali atau mengikut keperluan bagi memastikan dokumen sentiasa relevan.

K01/04 Pematuhan Dasar

PKS JPA mestilah dipatuhi oleh semua pengguna.

Semua Pengguna



ORGANISASI KESELAMATAN MAKLUMAT

KAWALAN

Polisi Keselamatan Siber JPA Versi 1.1

02



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

15 dari 128

Kawalan 02: Organisasi Keselamatan Maklumat

Objektif

Menerangkan peranan dan tanggungjawab semua pihak yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS JPA.

K02/01 Tadbir Urus Keselamatan Maklumat

K02/01/01 Ketua Pengarah Perkhidmatan Awam (KPPA)

Peranan dan tanggungjawab KPPA adalah seperti berikut:

KPPA

- a. memastikan semua keperluan jabatan seperti sumber kewangan, sumber kakitangan dan perlindungan keselamatan adalah mencukupi.

K02/01/02 Ketua Pegawai Maklumat (CIO)

Jawatan Ketua Pegawai Maklumat (CIO) adalah disandang oleh Timbalan Ketua Pengarah Perkhidmatan Awam (Operasi).

CIO

Peranan dan tanggungjawab CIO adalah seperti berikut:

- a. bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT JPA;
- b. bertanggungjawab menyelaras dan mengurus pelan tindakan dan program keselamatan seperti penyediaan PKS JPA, pelan latihan dan kesedaran pengguna, pengurusan risiko dan pengauditan; dan
- c. menentukan keperluan keselamatan ICT.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

16 dari 128

K02/01/03 Pegawai Keselamatan ICT (ICTSO)

Jawatan Pegawai Keselamatan ICT (ICTSO) adalah disandang oleh Pengarah Bahagian Pembangunan dan Pengurusan Maklumat Strategik (BPMS) JPA.

ICTSO

Peranan dan tanggungjawab ICTSO adalah seperti berikut:

- a. mempengerusikan Jawatankuasa Keselamatan ICT (JKICT);
- b. menguatkuasakan pelaksanaan PKS JPA di semua bahagian di JPA;
- c. memastikan pengurusan risiko dan audit keselamatan ICT berpandukan dokumen Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) dan PKS JPA;
- d. mencadangkan langkah-langkah pengukuhan bagi mematuhi dasar-dasar berkaitan keselamatan ICT JPA;
- e. melaporkan insiden keselamatan ICT kepada pihak *National Cyber Security Agency* (NACSA) dan seterusnya membantu dalam penyiasatan atau pemulihan;
- f. memastikan program kesedaran keselamatan ICT dilaksanakan;
- g. menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlaku ancaman



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

17 dari 128

kepada keselamatan ICT dan menyediakan khidmat nasihat serta langkah pemulihan yang bersesuaian;

- h. melaporkan insiden keselamatan ICT kepada CIO bagi insiden yang memerlukan Pengurusan Kesenambungan Perkhidmatan;
- i. memastikan pematuhan PKS JPA oleh pihak luaran yang memberi perkhidmatan ICT kepada JPA untuk tujuan pembekalan, pemasangan, penyelenggaraan dan sebagainya;
- j. menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan ICT;
- k. memastikan PKS JPA dikemas kini sesuai dengan arahan jabatan, peraturan semasa, perubahan teknologi, dan ancaman dalaman dan luaran; dan
- l. memastikan Pelan Strategik Pendigitalan (PSP) JPA mengandungi aspek keselamatan ICT.

K02/01/04 Pengurus ICT

Jawatan Pengurus ICT disandang oleh dua (2) orang pegawai iaitu Pengarah Bahagian Pembangunan dan Pengurusan Maklumat Strategik dan Ketua Kluster Inovasi Teknologi Pengurusan, INTAN.

Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:

- a. memastikan PKS JPA dilaksanakan dan dipatuhi di bahagian;

Pengurus ICT



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

18 dari 128

- b. memastikan semua pengguna di JPA mematuhi dasar, piawaian dan garis panduan keselamatan ICT, dan seterusnya melaporkan sebarang insiden berkaitan keselamatan ICT;
- c. mengkaji semula aspek-aspek keselamatan fizikal seperti kemudahan *backup* dan persekitaran pejabat yang perlu, dengan persetujuan ICTSO;
- d. melaksanakan keperluan PKS dalam operasi semasa seperti berikut:
 - i. pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu;
 - ii. pembelian atau peningkatan perisian dan sistem komputer;
 - iii. perolehan teknologi dan perkhidmatan komunikasi baharu;
 - iv. pelantikan pembekal, perunding atau rakan usaha sama; dan
 - v. menentukan pembekal, perunding atau rakan usaha sama menjalani tapisan keselamatan selaras dengan keperluan tahap perkhidmatan.
- e. memastikan bentuk ancaman keselamatan terkini dikenal pasti dan penemuan ancaman dilaporkan kepada ICTSO;
- f. menyemak dan mengesahkan garis panduan, prosedur dan tatacara bagi semua aplikasi yang dibangunkan di bahagian-bahagian agar mematuhi keperluan PKS JPA;



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

19 dari 128

- g. membangun, mengkaji semula dan mengemas kini pelan kontingensi dengan mengaktifkan Pelan Pemulihan Bencana (DRP);
- h. memastikan sistem kawalan capaian pengguna ke atas aset-aset ICT JPA dilaksanakan; dan
- i. memastikan aspek keselamatan maklumat dilaksanakan dalam setiap pengurusan projek.

K02/01/05 Pentadbir Sistem

Pentadbir Sistem terdiri daripada seperti berikut:

- a. Pentadbir Rangkaian Dan Keselamatan;
- b. Pentadbir Pangkalan Data;
- c. Pentadbir Portal (Web Master);
- d. Pentadbir Pusat Data;
- e. Pentadbir Sistem Aplikasi;
- f. Pentadbir E-mel; dan
- g. Pentadbir Media Sosial JPA
- h. Pegawai Aset ICT

Pentadbir Sistem

Pentadbir Rangkaian Dan Keselamatan

Peranan dan tanggungjawab Pentadbir Rangkaian Dan Keselamatan adalah seperti berikut:

- a. memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di JPA beroperasi sepanjang masa;
- b. memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna;

Pentadbir Rangkaian
Dan Keselamatan



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

20 dari 128

- 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 JPA secara tidak sah;
- 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.

Pentadbir Pangkalan Data

Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut:

- a. melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data;
- b. memastikan pangkalan data boleh digunakan pada setiap masa;

Pentadbir Pangkalan
Data



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

21 dari 128

- c. melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data;
- d. melaksanakan *data masking* dalam menyediakan data latihan;
- e. memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur;
- f. melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip PKS;
- g. melaksanakan proses perkemasan data (housekeeping) di dalam pangkalan data;
- h. memantau proses backup dan restoration ke atas pangkalan data; dan
- i. melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.

Pentadbir Portal (Web Master)

Peranan dan tanggungjawab Pentadbir Portal adalah seperti berikut:

- a. menerima kandungan portal yang telah disahkan kesahihan dan terkini daripada sumber yang sah;
- b. memantau prestasi capaian dan menjalankan penalaan prestasi untuk memastikan akses yang lancar;

Pentadbir Portal



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

22 dari 128

- c. memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, mencero boh dan mengubahsuai antara muka portal;
- d. mengasingkan kandungan dan aplikasi dalam talian untuk capaian secara Intranet dan Internet ke portal JPA;
- e. memastikan hanya maklumat yang bersifat terbuka dipaparkan di portal;
- f. memastikan reka bentuk portal dibangunkan dengan ciri-ciri keselamatan supaya tidak dicero boh;
- g. melaksanakan perkemasan keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di *web server*;
- h. memantau proses *backup* dan *restoration* ke atas kandungan dan aplikasi portal; dan
- i. melaporkan sebarang pelanggaran keselamatan portal kepada ICTSO.

Pentadbir Pusat Data

Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti berikut:

- a. memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat;
- b. memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data;

Pentadbir Pusat Data



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

23 dari 128

- c. menjadualkan dan melaksanakan proses *backup* dan *restoration* ke atas pangkalan data dan sistem secara berkala;
- d. menyediakan perancangan Pelan Pemulihan Bencana;
- e. memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan;
- f. melaporkan sebarang pelanggaran keselamatan Pusat Data JPA kepada ICTSO; dan
- g. memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa.

Pentadbir Sistem Aplikasi

Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut:

- a. mengkaji cadangan pembangunan, pembaikan, penyelarasan, pelaksanaan, pemantauan dan penyelenggaraan sistem di JPA;
- b. menyediakan dokumentasi sistem dan manual pengguna;
- c. memastikan *virus pattern*, *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi dikemaskini supaya terhindar daripada ancaman virus dan penggadam;
- d. mengehadkan capaian ke atas dokumentasi sistem bagi mengelakkan dari penyalahgunaannya;

Pentadbir Sistem
Aplikasi



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

24 dari 128

- e. memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas;
- f. memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya;
- g. mematuhi dan melaksanakan prinsip-prinsip PKS dalam pewujudan akaun pengguna ke atas setiap sistem aplikasi; dan
- h. melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi.

Pentadbir E-mel

Peranan dan tanggungjawab Pentadbir E-mel adalah seperti berikut:

- a. menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat;
- b. pentadbir e-mel boleh membekukan akaun pengguna berdasarkan peraturan atau polisi semasa;
- c. memastikan pengguna e-mel JPA berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel JPA dan Internet JPA

Pentadbir E-mel



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

25 dari 128

serta pelaksanaan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan.

- d. memastikan kemudahan membuat capaian e-mel melalui pelbagai peralatan ICT dan alat komunikasi;
- e. melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem e-mel; dan
- f. memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa.

Pentadbir Media Sosial JPA

Peranan dan tanggungjawab Pentadbir Media Sosial JPA adalah seperti berikut:

- a. mematuhi segala peraturan atau syarat-syarat yang digariskan oleh penyedia platform media sosial;
- b. mentadbir dan menyemak ketepatan serta sensitiviti maklumat dalam pengurusan kandungan (video, audio, gambar dan dokumen) dan komen mengikut etika media sosial semasa; dan
- c. melaporkan sebarang pelanggaran polisi atau etika penggunaan media sosial yang sedang berkuat kuasa kepada Ketua Komunikasi Korporat, JPA.

Pentadbir Media
Sosial JPA



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

26 dari 128

Pegawai Aset ICT

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

Pegawai Aset ICT

- a. memastikan pengurusan aset ICT Kerajaan dijalankan selaras dengan peraturan yang ditetapkan;
- b. memastikan penerimaan aset ICT Kerajaan dilaksanakan oleh pegawai yang dilantik oleh Ketua Jabatan/ Bahagian;
- c. memastikan semua aset ICT Kerajaan yang diterima, didaftarkan menggunakan Sistem Pemantauan Pengurusan Aset (SPA) dalam tempoh dua (2) minggu dari tarikh pengesahan penerimaan aset;
- d. 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;
- e. memastikan Daftar Aset ICT dikemas kini apabila berlaku penambahan/ penggantian/ naik-taraf aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira;
- f. memastikan semua aset ICT Kerajaan diberi tanda pengenalan dengan cara melabel tanda Hak Kerajaan Malaysia dan nama JPA/ Bahagian/ Agensi



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

27 dari 128

- berkenaan di tempat yang mudah dilihat dan sesuai pada aset berkenaan;
- g. memastikan semua aset ICT Kerajaan ditandakan dengan Nombor Siri Pendaftaran mengikut susunan yang ditetapkan;
 - h. memastikan senarai daftar induk aset ICT Kerajaan disediakan;
 - i. 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;
 - j. memastikan setiap kerosakan aset ICT Kerajaan dilaporkan untuk tujuan penyelenggaraan;
 - k. bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset ICT Kerajaan;
 - l. merancang, memantau dan memastikan pemeriksaan aset ICT Kerajaan dilaksanakan ke atas keseluruhan aset ICT Kerajaan sekurang-kurangnya sekali setahun; dan
 - m. memastikan setiap kes kehilangan aset ICT Kerajaan dilaporkan dan diuruskan dengan teratur.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

28 dari 128

K02/01/06 Pengguna

Pengguna terdiri daripada warga JPA dan pihak luaran yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan.

Pengguna

Peranan dan tanggungjawab pengguna adalah seperti berikut:

- a. Pengguna perlu membaca, memahami dan mematuhi PKS JPA;
- b. mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;
- c. menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat;
- d. melaksanakan prinsip-prinsip PKS dan menjaga kerahsiaan maklumat JPA;
- e. melaksanakan langkah-langkah perlindungan seperti berikut:
 - i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
 - ii. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
 - iii. menentukan maklumat sedia untuk digunakan;
 - iv. menjaga kerahsiaan kata laluan;



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

29 dari 128

- v. mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan;
 - vi. melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
 - vii. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.
- f. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;
- g. menghadiri program-program kesedaran mengenai keselamatan ICT; dan
- h. mengawal aktiviti penggunaan media sosial seperti di bawah:
- i. mengelakkan ketirisan maklumat;
 - ii. tidak memberi atau mendedahkan sebarang komen atau pernyataan atau isu yang menyentuh perkara-perkara yang boleh menjejaskan imej dan dasar kerajaan;
 - iii. tidak menyebarkan maklumat yang berbentuk fitnah, hasutan dan lucah atau cuba memprovokasi sesuatu isu yang menyalahi peraturan dan undang-undang atau perkara yang menyentuh sensitiviti individu atau kumpulan tertentu; dan
 - iv. tidak menggunakan saluran media sosial hingga mengganggu fokus dalam urusan kerja.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

30 dari 128

- i. menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber JPA seperti di **Lampiran 1**.

K02/01/07 Jawatankuasa Pemandu ICT (JPICT) JPA

Keanggotaan JPICT adalah seperti berikut:

CIO

Pengerusi:

CIO

Ahli:

- a. Pengarah Bahagian Perkhidmatan;
- b. Pengarah Bahagian Pembangunan Organisasi;
- c. Pengarah INTAN;
- d. Pengarah Bahagian Pembangunan Modal Insan;
- e. Pengarah Bahagian Khidmat Pengurusan;
- f. Pengarah Bahagian Saraan;
- g. Pengarah Bahagian Pasca Perkhidmatan;
- h. Pengarah Bahagian Penyelidikan, Perancangan dan Dasar;
- i. Pengarah Bahagian Pengurusan Psikologi;
- j. Pengarah Bahagian Pembangunan dan Pengurusan Maklumat Strategik;
- k. Timbalan Pengarah Kanan Bahagian Penyelidikan, Perancangan dan Dasar;
- l. Timbalan Pengarah Bahagian Pembangunan dan Pengurusan Maklumat Strategik;
- m. Ketua Kluster Inovasi Teknologi Pengurusan, INTAN;
- n. Ketua Unit Komunikasi Korporat ;
- o. Penasihat Undang-undang (PUU);
- p. Ketua Unit Audit Dalam;
- q. ICTSO; dan
- r. Ketua Unit Integriti.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

31 dari 128

Urus setia:

BPMS

Bidang kuasa:

- a. menetapkan arah tuju dan strategi ICT untuk pelaksanaan ICT JPA;
- b. merancang, menyelaraskan dan memantau pelaksanaan program atau projek ICT JPA;
- c. menyelaraskan dan menyeragamkan pelaksanaan ICT agar selari dengan Pelan Strategik Pendigital (PSP) JPA dan PSP Sektor Awam;
- d. meluluskan projek-projek ICT;
- e. mengikuti dan memantau perkembangan program ICT serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT;
- f. merancang dan menentukan langkah-langkah keselamatan ICT;
- g. mengemukakan perolehan ICT yang telah diluluskan di peringkat JPIC JPA kepada Jawatankuasa Teknikal ICT (JTICT) MAMPU untuk kelulusan;
- h. mengemukakan laporan kemajuan projek ICT yang diluluskan kepada JTICT MAMPU;
- i. menetapkan dasar dan prosedur pengurusan portal JPA; dan
- j. meluluskan dokumen PKS JPA.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

32 dari 128

K02/01/08 Jawatankuasa Keselamatan ICT (JKICT) JPA

Keanggotaan JKICT adalah seperti berikut:

ICTSO

Pengerusi:

ICTSO

Ahli:

- a. Ketua JPACERT;
- b. Pentadbir Pusat Data BPMS dan INTAN;
- c. Pentadbir Sistem (System Administrator) BPMS dan INTAN;
- d. Pentadbir Sistem Aplikasi BPMS dan INTAN;
- e. Pentadbir Rangkaian Dan Keselamatan (Network and Security Administrator) BPMS dan INTAN ;
- f. Pentadbir Portal (Web Master) BPMS dan INTAN;
- g. Pentadbir Pangkalan Data (Database Administrator) BPMS dan INTAN;
- h. Pegawai Meja Bantuan (Helpdesk Officer) BPMS dan INTAN;
- i. Perunding Latihan INTAN;
- j. Wakil Pegawai Keselamatan Jabatan JPA;
- k. Wakil Pasukan Pelaksana ISMS, BPMS; dan
- l. Wakil Pasukan Pelaksana ISMS, INTAN.

Urus setia:

BPMS

Bidang kuasa:

- a. menyelenggara dokumen PKS JPA;
- b. memantau tahap pematuhan PKS JPA;
- c. menilai aspek teknikal keselamatan projek-projek ICT;



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

33 dari 128

- d. membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam jabatan yang mematuhi keperluan PKS JPA;
- e. menyemak semula sistem ICT supaya sentiasa mematuhi keperluan keselamatan dari semasa ke semasa;
- f. menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT;
- g. memastikan PKS JPA selaras dengan dasar-dasar ICT kerajaan semasa;
- h. bekerjasama dengan JPACERT untuk mendapatkan maklum balas dan insiden untuk tindakan penyelenggaraan PKS JPA;
- i. membincang tindakan yang melibatkan pelanggaran PKS JPA;
- j. merancang dan menyelaraskan pensijilan ISMS seperti:
 - i. rancang struktur organisasi ISMS;
 - ii. rancang kursus kesedaran ISMS;
 - iii. rancang skop ISMS;
 - iv. melaksanakan analisis jurang;
 - v. merancang jadual perbatuan ISMS;
 - vi. membantu Pelaksana ISMS menyediakan pernyataan dasar ISMS, *Statement of Applicability* (SoA), penilaian risiko, *risk treatment plan*, kaedah pengukuran kawalan dan prosedur-prosedur ISMS; dan



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

34 dari 128

vii. permohonan pensijilan.

k. mengemukakan isu dan masalah ISMS, jika ada; dan

l. membantu mengukur keberkesanan kawalan dan pelaksanaan ISMS.

K02/01/09 Pasukan Tindak Balas Insiden Keselamatan ICT (JPACERT)

Keanggotaan JPACERT adalah seperti berikut:

Pengerusi:

TP(M)T, BPMS

Ahli :

- a. Pegawai Teknologi Maklumat BPMS dan INTAN; dan
- b. Penolong Pegawai Teknologi Maklumat BPMS dan INTAN.

Urus setia:

BPMS

Peranan dan tanggungjawab JPACERT adalah seperti berikut:

- a. menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden;
- b. merekod dan menjalankan siasatan awal insiden yang diterima;
- c. menangani tindak balas (response) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum;

TP(M)T, BPMS



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

35 dari 128

- d. menghubungi dan melaporkan insiden yang berlaku kepada ICTSO dan pihak NACSA sama ada sebagai *input* atau untuk tindakan seterusnya;
- e. merujuk agensi-agensi di bawah kawalannya untuk mengambil tindakan pemulihan dan pengukuhan; dan
- f. melaporkan sebarang maklum balas dan insiden keselamatan ICT kepada JKICT.

K02/01/10 Jawatankuasa Pelan Pemulihan Bencana (JKDRP) JPA

Keanggotaan JKDRP BPMS dan INTAN adalah seperti berikut:

Pengerusi:

TP(M)T, BPMS

Ahli:

- a. Pasukan Pengurusan Bencana ;
- b. Pasukan Sistem dan Operasi Pusat Data;
- c. Pasukan Rangkaian dan Keselamatan;
- d. Pasukan Aplikasi;
- e. Pasukan Pangkalan Data; dan
- f. Pasukan Meja Bantuan.

Urus setia:

BPMS

Bidang kuasa:

- a. membangunkan Dokumen Pelan Pemulihan Bencana (DRP);

TP(M)T, BPMS



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

36 dari 128

- b. menyediakan kemudahan pemulihan bencana atau Pusat Pemulihan Bencana (Disaster Recovery Centre);
- c. membuat penilaian ke atas masalah dan jangkaan akibat bencana;
- d. memaklumkan pengurusan atasan berkenaan bencana, kemajuan pemulihan bencana dan masalah;
- e. mengaktifkan prosedur pemulihan bencana;
- f. mengkoordinasi operasi pemulihan;
- g. memantau operasi pemulihan dan memastikan jadual pemulihan dipatuhi;
- h. mendokumentasikan operasi pemulihan; dan
- i. mengkoordinasi simulasi pemulihan bencana.

K02/02 Pihak Luaran

K02/02/01 Keperluan Keselamatan Dalam Perkhidmatan ICT

Pihak Luaran terdiri daripada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan atau pelawat yang mengunjungi JPA atas urusan rasmi.

Perkara yang perlu dipatuhi:

- a. mengenal pasti risiko ke atas keselamatan maklumat dan memastikan pelaksanaan kawalan yang sesuai ke atas maklumat tersebut;

Pengurus ICT,
Pentadbir Sistem



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

37 dari 128

- b. memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga;
- c. akses kepada aset ICT JPA perlu berlandaskan perjanjian dan peraturan yang telah ditetapkan. Perjanjian yang dimeterai perlu mematuhi perkara-perkara berikut:
 - i. PKS JPA;
 - ii. Tapisan Keselamatan;
 - iii. Arahan Teknologi Maklumat 2007 (IT Instructions);
 - iv. Perakuan Akta Rahsia Rasmi 1972; dan
 - v. Hak Harta Intelekt.
- d. melaksanakan keselamatan dan menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber JPA (Lampiran 1) serta Perakuan Akta Rahsia Rasmi 1972 bagi perakuan untuk tidak membocorkan sebarang maklumat rasmi yang diperoleh sepanjang berkhidmat dengan JPA seperti **Lampiran 4**; dan
- e. pihak luaran kategori pelawat sahaja dikecualikan daripada mematuhi peraturan a hingga d seperti di atas.



KESELAMATAN SUMBER MANUSIA

KAWALAN

Polisi Keselamatan Siber JPA Versi 1.1

03



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

39 dari 128

Kawalan 03: Keselamatan Sumber Manusia

Objektif

Memastikan semua pengguna yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.

K03/01 Sebelum Perkhidmatan

Memastikan semua pengguna yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuai, penipuan dan penyalahgunaan aset ICT.

Pengguna,
Pengurusan Sumber
Manusia

Perkara yang mesti dipatuhi termasuk yang berikut:

- menyatakan dengan lengkap dan jelas peranan dan tanggungjawab semua pengguna yang berkepentingan ke atas keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan
- menjalankan tapisan keselamatan, menandatangani Perakuan Akta Rahsia Rasmi 1972 dan Surat Akuan Pamatuan PKS untuk semua pengguna yang berkepentingan.

K03/02 Semasa Perkhidmatan

Memastikan semua pengguna yang berkepentingan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong

Pengguna,
Pengurusan Sumber
Manusia



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

40 dari 128

PKS JPA dan meminimumkan risiko kesilapan, kecuaiian, kecurian, penipuan dan penyalahgunaan aset ICT.

Perkara yang perlu dipatuhi termasuk yang berikut:

- a. memastikan semua pengguna yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan ditetapkan JPA;
- b. memastikan latihan dan program kesedaran yang diberikan kepada pengguna dari semasa ke semasa bagi meningkatkan kompetensi pengguna berkaitan keselamatan aset ICT;
- c. memastikan prosedur latihan jabatan sentiasa dikemas kini bersesuaian dengan fungsi tugas semasa setiap pengguna;
- d. memastikan adanya tindakan tatatertib/ atau perundangan ke atas semua pengguna sekiranya berlaku pelanggaran keselamatan maklumat jabatan; dan
- e. mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

K03/03 Bertukar Atau Tamat Perkhidmatan

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

Perkara yang perlu dipatuhi termasuk:

Pengguna,
Pengurusan Sumber
Manusia



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

41 dari 128

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



PENGURUSAN ASET

KAWALAN

Polisi Keselamatan Siber JPA Versi 1.1

04



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

42 dari 128

Kawalan 04: Pengurusan Aset

Objektif

Memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT JPA.

K04/01 Akauntabiliti Aset ICT

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

Pegawai Aset ICT,
Pengguna

Tanggungjawab yang perlu dipatuhi untuk memastikan semua aset ICT dikawal dan dilindungi:

- memastikan semua aset ICT dikenal pasti, dikelaskan, didokumenkan, diselenggarakan dan dilupuskan. Maklumat aset direkodkan dan dikemas kini dalam Sistem Pengurusan Aset (SPA), Kad Daftar Harta Modal dan Aset Alih Bernilai Rendah sebagaimana mengikut Pekeliling Perbendaharaan AM 2 Tahun 2018: Tatacara Pengurusan Aset Alih Kerajaan atau senarai aset yang berkaitan;
- memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;
- memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di JPA;
- memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan;



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

43 dari 128

- e. setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalan atau milikan; dan
- f. penggunaan aset ICT JPA mestilah untuk tujuan tugas rasmi sahaja.

K04/02 Peminjaman dan Pemulangan Aset ICT

Peminjaman

Langkah-langkah perlu diambil termasuklah seperti berikut:

- 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 status perkhidmatan pegawai yang :

- a. bertukar keluar;
- b. bersara;

Pegawai Aset ICT



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

44 dari 128

c. ditamatkan perkhidmatan; dan

d. diarahkan oleh Ketua Jabatan

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

K04/03 Pengelasan Maklumat

Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada JPA. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan dan dilabel sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut:

- a. Rahsia Rasmi;
 - i. Rahsia Besar
 - ii. Rahsia
 - iii. Sulit
 - iv. Terhad
- b. Rasmi; dan
- c. Data terbuka.

Pegawai Pengelas

K04/04 Pengendalian Maklumat

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampaikan, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut:

Semua



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

45 dari 128

- a. menghalang pendedahan atau potensi ketirisan 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 piawaian, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan;
- f. melaksanakan peraturan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;
- g. menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum; dan
- h. mewujudkan salinan pendua maklumat penting bagi mengurangkan risiko kehilangan dan kemusnahan.

K04/05 Pengelasan dan Pengendalian Data Terbuka

Data Terbuka ialah data yang bebas digunakan, dikongsi dan digunakan semula oleh orang awam, agensi Kerajaan dan organisasi swasta untuk pelbagai tujuan.

Jabatan akan menyediakan set data terbuka berdasarkan bidang atau sektor atau kluster. Kategori set data ini tidak terhad dan boleh berubah mengikut fungsi teras dan keperluan semasa Jabatan.

Semua



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

46 dari 128

Data terbuka yang telah diperakukan oleh Jabatan akan dikemukakan ke JPM untuk kelulusan dan seterusnya diterbitkan ke Portal Data Terbuka Sektor Awam (DTSA) di bawah pengurusan MAMPU.

K04/06 Pengendalian Media

K04/06/01 Media Storan

Media storan merupakan peralatan yang digunakan untuk menyimpan data dan maklumat seperti *optical disk, flash disk, hard disk, USB flash drive, catridge tape, compact disc (CD)* dan media storan lain.

Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan ketersediaan untuk digunakan.

Bagi menjamin keselamatan, langkah-langkah berikut perlu diambil:

- semua media storan perlu dikawal bagi mencegah daripada capaian yang tidak dibenarkan, kecurian dan kemusnahan;
- bagi media storan yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu;
- semua media storan yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat;
- semua media storan yang mengandungi data/maklumat kritikal hendaklah disimpan di dalam peti keselamatan (data safe) yang mempunyai ciri-ciri

Pentadbir Sistem,
Pegawai Aset ICT



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

47 dari 128

ketahanan daripada dipecahkan, api, air dan medan magnet;

- e. storan dan peralatan *backup* hendaklah disimpan di lokasi yang selamat. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja;
- f. akses dan pergerakan kepada media storan perlu direkodkan;
- g. peralatan *backup* hendaklah diletakkan di tempat yang selamat dan terhad kepada pengguna yang dibenarkan sahaja; dan
- h. sebarang kehilangan media storan yang berlaku hendaklah dilaporkan mengikut Prosedur Pelaporan Insiden.



KAWALAN CAPAIAN

KAWALAN

Polisi Keselamatan Siber JPA Versi 1.1

05



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

48 dari 128

Kawalan 05: Kawalan Capaian

Objektif

Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT.

K05/01 Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong kawalan capaian pengguna sedia ada.

Pentadbir Sistem

K05/02 Pengurusan Capaian Pengguna

K05/02/01 Pendaftaran Pengguna

Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, Pentadbir Sistem perlu mengambil langkah-langkah berikut:

- akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan;
- akaun *user id* hendaklah mencerminkan identiti pengguna;
- pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika kaedah penggunaannya melanggar peraturan;
- penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan

Pentadbir Sistem,
Pengguna



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

49 dari 128

e. Pemilik akaun dan capaian pengguna adalah tertakluk kepada peraturan jabatan dan tindakan pengemaskinian atau pembatalan hendaklah diambil atas sebab berikut:

- i. pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi sebulan;
- ii. bertukar bidang tugas kerja;
- iii. bertukar ke agensi lain;
- iv. bersara; atau
- v. ditamatkan perkhidmatan.

K05/02/02 Hak Capaian

Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat, atas prinsip perlu mengetahui (need-to-know-basis).

Keperluan capaian hendaklah sentiasa dipantau dan dikemas kini bagi memastikan hak capaian ini diberikan kepada pegawai dan kakitangan yang dibenarkan sahaja.

Pentadbir Sistem

K05/02/03 Pengurusan Kata Laluan

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh JPA seperti berikut:

- a. dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;

Pentadbir Sistem
Pengguna



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

50 dari 128

- b. panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan antara huruf dan nombor (alphanumeric) dan aksara khas;
- c. kekerapan penukaran dan penggunaan kata laluan adalah mengikut ketetapan polisi pengurusan kata laluan yang berkuat kuasa;
- d. kata laluan sistem pengoperasian (OS) atau *Directory Service* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;
- e. kata laluan tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun;
- 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. had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum tiga (3) kali sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula;
- j. kata laluan hendaklah disimpan dalam bentuk yang telah disulitkan (encrypted) dan selamat ;



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

51 dari 128

- k. penggunaan atribut *Remember Me* adalah tidak dibenarkan sama sekali. Sekiranya akaun atau kata laluan disyaki telah dicerobohi, maka laporan kejadian hendaklah dilaporkan kepada pasukan JPACERT dan tindakan menukar kata laluan perlu dilakukan;
- l. kata laluan hendaklah ditukar apabila disyaki berlakunya kebocoran atau dikompromi (compromised); dan
- m. sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.

K05/03 Capaian Sistem Pengoperasian

K05/03/01 Capaian Sistem Pengoperasian

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan.

Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian terhadap sistem komputer. Kemudahan ini juga perlu bagi:

- a. mengenal pasti identiti/terminal/lokasi bagi setiap pengguna yang dibenarkan;
- b. merekodkan capaian yang berjaya dan gagal; dan
- c. membolehkan pengesahan kata laluan dilaksanakan berdasarkan kriteria kata laluan yang kukuh.

Pentadbir
Sistem



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

52 dari 128

Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut:

- a. mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan;
- b. mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*;
- c. menjana amaran (alert) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem; dan
- d. menyediakan tempoh penggunaan mengikut kesesuaian.

Perkara-perkara yang perlu dipatuhi termasuk berikut:

- a. mengawal capaian ke atas sistem operasi menggunakan prosedur *log on* yang terjamin;
- b. mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja dan satu teknik pengesahan yang bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna;
- c. mewujudkan fungsi pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah kukuh mengikut polisi kata laluan yang berkuat kuasa;
- d. mengehadkan dan mengawal penggunaan program utiliti yang berkemampuan bagi satu tempoh yang ditetapkan; dan



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

53 dari 128

e. mengehendkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.

K05/03/02 Token/Sijil Digital

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 pihak yang mengeluarkan token.

Pengguna

K05/04 Capaian Aplikasi dan Maklumat

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

Capaian sistem dan aplikasi di JPA adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut perlu dipatuhi:

Pentadbir
Sistem



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

54 dari 128

- a. pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan;
- b. setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini;
- c. menyediakan paparan dasar privasi/notis penafian kepada pengguna ketika menggunakan aplikasi bagi melindungi maklumat daripada sebarang bentuk penyalahgunaan;
- d. memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah;
- e. maklumat tarikh *login* terakhir hendaklah direkodkan; dan
- f. digalakkan *session timeout* dilaksanakan.

K05/05 Capaian Jarak Jauh

- a. capaian jarak jauh yang dimaksudkan merangkumi:
 - i. capaian daripada sistem rangkaian dalaman; dan
 - ii. capaian daripada sistem rangkaian luaran bagi lokasi luar pejabat untuk tujuan *teleworking*.
- b. penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi (encryption);

Pentadbir Sistem,
Pengguna



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

55 dari 128

- c. lokasi bagi akses ke sistem ICT JPA hendaklah dipastikan selamat;
- d. penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pentadbir Rangkaian dan Keselamatan. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini; dan
- e. capaian jarak jauh hendaklah menggunakan kemudahan yang disediakan oleh jabatan.

K05/06 Kawalan Capaian Rangkaian

K05/06/01 Capaian Rangkaian

Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

- a. mewujudkan segmen rangkaian yang bersesuaian bagi membezakan di antara rangkaian JPA dan rangkaian awam;
- b. mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dengan peralatan yang menepati kesesuaian penggunaannya;
- c. memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT;
- d. capaian pengguna jarak jauh (remote user) perlulah dikawal dan dipantau;

Pentadbir Rangkaian
dan Keselamatan



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

56 dari 128

- e. capaian fizikal dan logikal ke atas peralatan rangkaian bagi tujuan mengubah konfigurasi perlulah dikawal; dan
- f. semua rangkaian yang dikongsi (shared networks), terutama yang keluar daripada rangkaian JPA, polisi perlu diwujudkan untuk mengawal capaian oleh pengguna.

K05/06/02 Capaian Internet

- a. penggunaan Internet di JPA hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian dan Keselamatan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kawalan ini akan dapat melindungi daripada sebarang bentuk ancaman ke atas rangkaian JPA;
- b. penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;
- c. polisi *Content Filtering* mestilah digunakan dan dipantau bagi mengawal akses Internet. Pengguna boleh memohon pengecualian mengikut fungsi kerja untuk pertimbangan;
- d. penggunaan teknologi (packet shaper) adalah perlu bagi menguruskan penggunaan *bandwidth* yang maksimum dan lebih berkesan; dan
- e. penggunaan kemudahan Internet peribadi di pejabat seperti modem, *hotspot* dan sebagainya untuk tujuan

Pentadbir Rangkaian
dan Keselamatan

Pengurus ICT

Pentadbir Rangkaian
dan Keselamatan



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

57 dari 128

sambungan ke Internet adalah tidak dibenarkan kecuali mendapat kelulusan Ketua Jabatan melalui borang permohonan seperti di **Lampiran 3**.

K05/07 Peralatan Mudah Alih

Perkara yang perlu dipatuhi adalah seperti berikut:

- merekodkan aktiviti keluar masuk penggunaan peralatan mudah alih bagi mengesan pergerakan peralatan tersebut daripada kehilangan atau kerosakan;
- peralatan mudah alih hendaklah disimpan atau dikunci di tempat yang selamat apabila tidak digunakan; dan
- memastikan peralatan mudah alih yang dibawa keluar dari pejabat perlu disimpan dan dijaga dengan baik bagi mengelakkan daripada kecurian.

Pegawai Aset ICT,
Pengguna

K05/08 Bring Your Own Device (BYOD)

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 JPA.

Sebagai garis panduan, pengguna bertanggungjawab memastikan langkah-langkah keselamatan perlindungan berkaitan penggunaan BYOD seperti berikut:

Pengguna



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

58 dari 128

- 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:

- 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 KRIPTOGRAFI

KAWALAN

Polisi Keselamatan Siber JPA Versi 1.1

06



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

59 dari 128

Kawalan 06: Kawalan Kriptografi

Objektif

Melindungi kerahsiaan, integriti dan kesahihan maklumat yang merangkumi data dalam sistem rangkaian, sistem aplikasi dan pangkalan data.

K06/01 Kriptografi

Kunci enkripsi mestilah dilindungi dengan menggunakan cara kawalan yang terbaik dan hendaklah dirahsiakan. Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut.

Pentadbir Sistem,
Pengguna

Kriptografi turut merangkumi kaedah-kaedah seperti berikut:

- Kesemua pelaksanaan sistem hendaklah menggunakan ID atau kata laluan dan dibuat enkripsi.
- Penggunaan PKI (Public Key Infrastructure) yang selamat yang dibekalkan oleh Kerajaan.

K06/01/01 Enkripsi

Kesemua pelaksanaan sistem hendaklah menggunakan ID dan kata laluan, dan dibuat enkripsi.

Pentadbir Sistem,
Pengguna

K06/01/02 Public Key Infrastructure (PKI)

Penggunaan PKI yang selamat yang dibekalkan oleh Kerajaan.

Pentadbir Sistem,
Pengguna



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

60 dari 128

K06/01/03 Tandatangan Digital

Penggunaan tandatangan digital digalakkan digunakan di dalam sistem bagi pengguna yang melaksanakan transaksi secara elektronik.

Pentadbir Sistem,
Pengguna



KESELAMATAN FIZIKAL & PERSEKITARAN

KAWALAN

Polisi Keselamatan Siber JPA Versi 1.1

07



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

61 dari 128

Kawalan 07: Keselamatan Fizikal dan Persekitaran

Objektif

Melindungi premis dan aset ICT daripada sebarang bentuk ancaman dan pencerobohan yang boleh mengakibatkan kerosakan, kehilangan dan gangguan perkhidmatan ICT.

K07/01 Keselamatan Kawasan

K07/01/01 Kawasan Larangan Lokasi ICT

Kawasan larangan lokasi ICT bagi JPA ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga JPA yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis tersebut. Kawasan larangan lokasi ICT JPA adalah Pusat Data JPA.

Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas premis tersebut adalah seperti berikut:

- sumber data atau *server*, peralatan komunikasi dan storan perlu ditempatkan di pusat data yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegah kebakaran;
- akses adalah terhad kepada warga JPA yang telah diberi kuasa sahaja dan dipantau pada setiap masa;
- pemantauan dibuat menggunakan Sistem CCTV atau peralatan-peralatan lain yang sesuai;
- peralatan keselamatan seperti CCTV dan pengimbas biometrik perlu diperiksa secara berjadual;

Pentadbir Pusat Data



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

62 dari 128

- e. butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan;
- f. pihak luaran yang dibawa masuk mesti diawasi atau diiringi oleh pegawai bertanggungjawab di sepanjang tempoh di lokasi mengikut keperluan sewajarnya;
- g. lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggaran dan laluan awam;
- h. memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan;
- i. memperkukuhkan dinding dan siling; dan
- j. mengehadkan jalan keluar masuk.

K07/01/02 Kawalan Masuk Fizikal

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- a. Warga JPA
 - i. semua warga hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; dan
 - ii. semua pas keselamatan hendaklah diserahkan kembali kepada JPA apabila pengguna berhenti atau bersara.
- b. Pelawat
 - i. setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu masuk utama

Pengguna / Pelawat



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

63 dari 128

premis-premis JPA. Pas ini hendaklah dikembalikan semula selepas tamat lawatan.

c. Kehilangan Pas Keselamatan

- i. kehilangan pas mestilah dilaporkan dengan segera.

K07/02 Keselamatan Peralatan

K07/02/01 Peralatan ICT

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;
- pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran peralatan dan konfigurasi yang telah ditetapkan;
- pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem;
- pengguna mesti memastikan perisian antivirus bagi semua peralatan ICT yang dibekalkan oleh Jabatan seperti komputer peribadi, *notebook*, *server* dan lain-lain yang berada di bawah tanggungjawab mereka sentiasa aktif (activated) dan dikemas kini di samping turut melakukan imbasan ke atas media storan yang digunakan;

Pengguna, Pentadbir Sistem, Pegawai Aset ICT, Penyelaras ICT Bahagian



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

64 dari 128

- e. semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, kerosakan, pengubahsuaian tanpa kebenaran dan penyalahgunaan;
- f. aset ICT hendaklah disimpan di tempat yang selamat dan sentiasa di bawah kawalan pegawai yang bertanggungjawab. Arahan Keselamatan Kerajaan hendaklah sentiasa dipatuhi bagi mengelak berlakunya kerosakan atau kehilangan aset;
- g. sekiranya peralatan ICT tidak digunakan, peralatan tersebut hendaklah disimpan di dalam almari atau kabinet atau peti besi atau stor atau bilik khas yang berkunci untuk penyimpanan peralatan ICT;
- h. peralatan ICT yang kritikal perlu disokong oleh UPS;
- i. UPS yang berkuasa tinggi perlu diletakkan di bilik yang berasingan bersuhu rendah yang dilengkapi dengan pengudaraan yang sesuai;
- j. semua peralatan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switch*, *router* dan lain-lain perlu diletakkan di dalam bilik atau rak berkunci;
- k. semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai;



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

65 dari 128

- l. peralatan ICT yang hendak dibawa keluar dari premis JPA, perlulah mendapat kelulusan Pegawai Aset ICT atau Penyelaras ICT Bahagian bagi tujuan pemantauan; dan
- m. aset ICT yang hilang hendaklah dilaporkan mengikut pekeliling perbendaharaan sedia ada.

K07/02/02 *Clear Desk dan Clear Screen*

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

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- a. menggunakan kemudahan *password screen saver* atau *log out* apabila meninggalkan komputer;
- 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.

Pengguna

K07/02/03 *Media Tandatangan Digital*

Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah-langkah berikut:

Pentadbir Sistem,
Pengguna



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

66 dari 128

- a. pengguna hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;
- b. tidak boleh dipindah milik atau dipinjamkan; dan
- c. sebarang kehilangan yang berlaku hendaklah dilaporkan kepada pihak yang dipertanggungjawabkan.

K07/02/04 Perisian Dan Aplikasi

Sebarang perisian dan aplikasi yang digunakan hendaklah mematuhi langkah-langkah berikut:

- a. hanya perisian yang rasmi sahaja dibenarkan bagi kegunaan jabatan;
- b. lesen perisian perlu disimpan di tempat yang selamat dan dikawal capaiannya;
- c. kod sumber (source code) sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan; dan
- d. sistem aplikasi, perisian dan kod sumber tidak dibenarkan dikongsi, diagih, dibawa keluar atau didemonstrasikan kepada pihak lain kecuali dengan kebenaran Pengurus ICT.

Pengurus ICT,
Pegawai Aset ICT,
Pentadbir Sistem



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

67 dari 128

K07/02/05 Peralatan Tanpa Penyeliaan (Unattended Equipment)

	Pengguna perlu memastikan mana-mana peralatan yang ditinggalkan tanpa penyeliaan mematuhi ciri-ciri keselamatan seperti mempunyai kata laluan dan sebagainya. Peralatan hendaklah diselenggarakan dengan betul bagi memastikan ketersediaan, kerahsiaan dan integriti.	Pengguna
--	--	----------

K07/02/06 Peralatan di Luar Premis

	Peralatan yang dibawa keluar dari premis JPA adalah terdedah kepada pelbagai risiko. Peralatan yang dibawa keluar premis JPA merangkumi: a. penggunaan peralatan secara sementara bagi keperluan mesyuarat, latihan dan sebagainya; dan b. penempatan peralatan secara kekal di sesebuah agensi lain. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. peralatan perlu dilindungi dan dikawal sepanjang masa; dan b. penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Pentadbir Sistem
--	---	------------------



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

68 dari 128

K07/02/07 Pelupusan

Aset ICT yang hendak dilupuskan perlu mematuhi tatacara pelupusan semasa. Langkah-langkah berikut perlu diambil dalam memastikan peralatan ICT JPA dilupuskan dengan teratur iaitu:

Pegawai Aset ICT,
Pengguna

- a. pegawai aset ICT akan mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;
- b. peralatan yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaskan;
- c. data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal;
- d. pelupusan peralatan ICT boleh dilakukan secara berpusat atau tidak berpusat mengikut tatacara pelupusan semasa yang berkuat kuasa;
- e. sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan sandar;
- f. maklumat lanjut berhubung pelupusan boleh dirujuk kepada pekeliling perbendaharaan semasa yang berkuat kuasa; dan
- g. pelupusan dokumen dan rekod hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

69 dari 128

K07/02/08 Penyelenggaraan

Peralatan hendaklah diselenggarakan dengan betul bagi memastikan ketersediaan, kerahsiaan dan integriti.

Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut:

- a. mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua peralatan yang di selenggara;
- b. memastikan peralatan hanya diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja;
- c. menyemak dan menguji semua peralatan 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

K07/03 Kawalan Persekitaran

K07/03/01 Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk perolehan, menyewa, mengubahsuai, pembelian hendaklah dirujuk terlebih dahulu ke Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK).
Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil:

- a. merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan

Pengurus ICT



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

70 dari 128

- komputer dan ruang atur pejabat dan sebagainya) dengan teliti;
- b. semua ruang pejabat khususnya yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;
 - c. peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;
 - d. bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT;
 - e. semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT;
 - f. pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan
 - g. semua peralatan perlindungan keselamatan dan kebakaran hendaklah di selenggara bagi memastikan ia dapat berfungsi dengan baik.

K07/03/02 Kabel Rangkaian

- a. semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat;

Pentadbir Rangkaian



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

71 dari 128

- b. menggunakan kabel mengikut spesifikasi yang telah ditetapkan; dan
- c. melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*.

K07/03/03 Bekalan Kuasa

Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan bekalan kuasa:

- a. semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT;
- b. peralatan sokongan seperti UPS dan penjana kuasa (power generator) boleh digunakan bagi perkhidmatan kritikal seperti di bilik *server* supaya mendapat bekalan kuasa berterusan; dan
- c. semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual oleh pihak penyelenggara bangunan.

Pengurus ICT

K07/03/04 Prosedur Kecemasan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a. setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Pelan Tindakan dan Kecemasan JPA; dan

Pengguna,
Pegawai Keselamatan
Kebakaran



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

72 dari 128

- b. kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Kebakaran yang dilantik mengikut aras.

K07/03/05 Mekanisme Pelaporan Insiden Bukan ICT

Semua pengguna yang terlibat haruslah melaporkan dan merekodkan sebarang kejadian atau kerosakan peralatan bukan ICT kepada pihak pentadbiran bahagian.

Semua Pengguna

K07/03/06 Mekanisme Kawalan Peralatan Sewaan/Ujicuba (Proof Of Concept)

a. Penerimaan

- i. peralatan yang diterima bebas daripada virus, *backdoor*, *worm* dan perkara-perkara yang boleh memberi ancaman kepada perkhidmatan ICT jabatan.

Pentadbir Sistem

b. Penyelenggaraan

- i. capaian melalui rangkaian luar JPA adalah tidak dibenarkan; dan
ii. aktiviti penyelenggaraan adalah di bawah pengawasan pegawai JPA.

c. Pemulangan

- i. maklumat yang tersimpan dalam storan perlu dihapuskan secara kekal (secured delete); dan
ii. memastikan semua maklumat jabatan tidak tertinggal pada peralatan.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

73 dari 128

K07/04 Keselamatan Sistem Dokumentasi

Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan sistem dokumentasi:

- a. memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;
- b. mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada;
- c. setiap dokumen hendaklah difailkan dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;
- d. pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan;
- e. kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; dan
- f. menggunakan enkripsi (encryption) ke atas dokumen rahsia rasmi yang disediakan, disimpan dan dihantar secara elektronik.

Pentadbir Sistem,
Pentadbir Fail



KESELAMATAN OPERASI

KAWALAN

Polisi Keselamatan Siber JPA Versi 1.1

08



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

74 dari 128

Kawalan 08: Keselamatan Operasi

Objektif

Memastikan pengurusan operasi dan kemudahan pemprosesan maklumat berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

K08/01 Prosedur Operasi

K08/01/01 Pengendalian Dokumen Prosedur Operasi

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- semua prosedur operasi ICT yang diwujudkan, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal;
- setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap; dan
- semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.

Pentadbir Sistem

K08/01/02 Pengurusan Perubahan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- pengubahsuaian melibatkan peralatan, sistem pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran Pengurus ICT, pegawai atasan atau pemilik aset ICT terlebih dahulu;

Pentadbir Sistem



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

75 dari 128

- b. aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;
- c. semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan
- d. semua aktiviti perubahan atau pengubahsuaian hendaklah direkodkan dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau sebaliknya.

K08/01/03 Pengasingan Tugas dan Tanggungjawab

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a. skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;
- b. tugas mewujudkan, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah dilakukan oleh pegawai yang berlainan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan

Pengurus ICT,
Pentadbir Sistem



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

76 dari 128

- c. peralatan dan rangkaian yang digunakan bagi tugas membangun, mengemas kini, dan menguji aplikasi hendaklah diasingkan dari peralatan dan rangkaian yang digunakan di dalam persekitaran pembangunan dan pengujian; peringkat persediaan dan produksi.

K08/02 Perancangan dan Penerimaan Sistem

K08/02/01 Perancangan Kapasiti

- a. kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan
- b. keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

Pentadbir Sistem

K08/02/02 Penerimaan Sistem

Semua sistem baharu (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.

Pentadbir Sistem

K08/03 Perlindungan dari Perisian Berbahaya

K08/03/01 Perlindungan dari Perisian Berbahaya

Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT dari perisian berbahaya:

- a. memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus,

Pentadbir Sistem,
Pengguna



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

77 dari 128

Intrusion Detection System (IDS) dan *Intrusion Prevention System* (IPS) mengikut prosedur penggunaan yang betul dan selamat;

- b. memasang dan menggunakan hanya perisian yang tulen;
- c. mengimbas semua perisian, sistem, media storan dan kepilang fail dengan antivirus yang telah disediakan oleh Jabatan sebelum menggunakannya;
- d. memastikan paten antivirus pada peralatan ICT dikemas kini dengan versi terkini;
- e. menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diinginkan seperti kehilangan dan kerosakan maklumat;
- f. menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;
- g. memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; dan
- h. mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

78 dari 128

K08/03/02 Perlindungan dari *Mobile Code*

Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.

Pengguna

K08/04 *Housekeeping*

K08/04/01 *Backup*

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana/insiden, *backup* seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. *Backup* hendaklah direkodkan dan disimpan di *off site*, di antaranya adalah:

- membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaharu;
- membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi;
- menguji sistem *backup* sedia ada dan bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan
- backup* dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan *backup* bergantung pada tahap kritikal maklumat dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi.

Pentadbir Sistem



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

79 dari 128

K08/05 Pengurusan Media

K08/05/01 Media Storan Mudah Alih

Penghantaran atau pemindahan media storan mudah alih yang mengandungi maklumat terperingkat ke luar pejabat hendaklah mendapat kebenaran daripada Pengurus ICT terlebih dahulu.

Pengguna

K08/05/02 Prosedur Pengendalian Media

Di antara prosedur-prosedur pengendalian media termasuk:

- melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;
- mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;
- mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;
- mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan
- media yang mengandungi maklumat terperingkat hendaklah dihapus atau dimusnahkan mengikut peraturan dan prosedur yang betul dan selamat.

Pentadbir Sistem,
Pengguna



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

80 dari 128

K08/06 Paparan Maklumat Umum

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat umum adalah seperti berikut:

Pengguna

- memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu;
- memastikan segala maklumat yang hendak dipaparkan telah disahkan dan diluluskan sebelum dimuat naik ke portal; dan
- memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian.

K08/07 Pemantauan

K08/07/01 Pemantauan

Bertujuan untuk memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan, di antaranya seperti berikut:

Pentadbir Sistem

- log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;
- prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala;
- kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

81 dari 128

- d. kesalahan, kesilapan atau penyalahgunaan perlu dilog, dianalisis dan diambil tindakan sewajarnya; dan
- e. masa yang berkaitan dengan sistem pemprosesan maklumat dalam JPA perlu diselaraskan dengan sumber masa yang dipersetujui.

K08/07/02 Pengauditan dan Forensik ICT

JPACERT mestilah bertanggungjawab merekod dan menganalisis:

- a. sebarang percubaan pencerobohan kepada sistem ICT JPA;
- b. serangan kod perosak (malicious code), halangan pemberian perkhidmatan (denial of service), *spam*, pemalsuan (forgery), pencerobohan (intrusion) ancaman (threats) dan kehilangan fizikal (physical loss);
- c. pengubahsuaian ciri-ciri peralatan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;
- d. aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan;
- e. aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;
- f. aktiviti instalasi dan penggunaan perisian yang membebaskan *bandwidth* rangkaian;

JPACERT, ICTSO,
Pentadbir Sistem,



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

82 dari 128

- g. aktiviti penyalahgunaan akaun e-mel; dan
- h. aktiviti penukaran *IP address* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Rangkaian.

Langkah-langkah yang perlu diambil adalah seperti berikut:

- a. JPACERT akan menentukan prosedur pengumpulan bahan bukti yang berkenaan bagi memastikan kesahihan ke atas sesuatu laporan yang akan disediakan;
- b. proses forensik dan pengauditan aset ICT mestilah dilakukan di tempat yang selamat;
- c. sekiranya hasil siasatan mensabitkan kesalahan kepada tertuduh, format laporan khas perlu disediakan; dan
- d. semua proses dan hasil siasatan adalah SULIT.

K08/07/03 Jejak Audit

Setiap sistem mestilah mempunyai jejak audit. 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 ciri-ciri berikut:

- a. rekod setiap aktiviti transaksi;

Pentadbir Sistem



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

83 dari 128

- 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 seperti yang disarankan oleh Akta Arkib Negara.

Pentadbir Sistem 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 daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.

K08/07/04 Sistem Log

Fail log hendaklah disimpan untuk tempoh sekurang-kurangnya enam (6) bulan. Jenis fail log bagi *server* dan aplikasi yang perlu diaktifkan adalah seperti berikut:

- i. Fail log sistem pengoperasian;
- ii. Fail log servis (web, e-mel);
- iii. Fail log aplikasi (audit trail); dan
- iv. Fail log rangkaian (switch, firewall, IPS)

Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:

Pentadbir Sistem



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

84 dari 128

- a. mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;
- b. menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaiki pulih dengan segera; dan
- c. sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.

K08/07/05 Penyeragaman Waktu (Time Synchronisation)

Waktu bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal.

Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam JPA atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh National Metrology Institute of Malaysia (NMIM).

Pentadbir Sistem

K08/07/06 Kawalan Pengoperasian Perisian

Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi bagi menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti yang berikut:

Pentadbir Sistem



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

85 dari 128

- a. strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian;
- b. aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; dan
- c. setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.

K08/07/07 Pengurusan Kerentanan Teknikal

Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan.

Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem aplikasi dan operasi yang digunakan bagi memastikan kawalan kerentanan teknikal adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya. Perkara yang perlu dipatuhi adalah seperti yang berikut:

- a. melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi;
- b. menganalisis tahap risiko kerentanan; dan

Pentadbir Sistem



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

86 dari 128

c. mengambil tindakan pengolahan dan kawalan risiko.



KESELAMATAN KOMUNIKASI

KAWALAN

Polisi Keselamatan Siber JPA Versi 1.1

09



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

87 dari 128

Kawalan 09: Keselamatan Komunikasi

Objektif

Memastikan sistem yang dibangunkan sendiri atau oleh pihak pembekal mempunyai ciri-ciri keselamatan maklumat dan komunikasi yang bersesuaian.

K09/01 Pengurusan Rangkaian

Infrastruktur Rangkaian perlu dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi dalam rangkaian.

Langkah-langkah bagi menangani ancaman ke atas rangkaian adalah seperti berikut:

- semua tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;
- capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;
- semua capaian kepada Internet dan sistem aplikasi mestilah melalui *firewall*;
- memasang perisian IPS bagi mengesan dan menghalang sebarang cubaan mencerooboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat JPA;

Pentadbir Rangkaian



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

88 dari 128

- e. memasang *Web Content Filter* untuk menyekat aktiviti yang dilarang; dan
- f. sebarang penyambungan rangkaian yang bukan di bawah kawalan JPA adalah tidak dibenarkan.

K09/02 Pengurusan Penghantaran dan Penerimaan Maklumat

Bertujuan untuk memastikan keselamatan penghantaran dan penerimaan maklumat dan perisian dalam agensi dan mana-mana entiti luar terjamin.

Pentadbir Sistem

Langkah-langkah bagi menjamin keselamatan penghantaran dan penerimaan maklumat adalah seperti berikut:

- a. polisi, prosedur dan kawalan penghantaran dan penerimaan maklumat yang formal perlu diwujudkan untuk melindungi maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;
- b. perjanjian perlu diwujudkan untuk penghantaran dan penerimaan maklumat dan perisian di antara JPA dengan pihak luar;
- c. media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan dan penerimaan;
- d. maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya; dan



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

89 dari 128

- e. polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem maklumat JPA.

K09/03 Pengurusan Mel Elektronik (E-mel)

Penggunaan e-mel di JPA hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet. Di antara prosedur-prosedur pengurusan e-mel termasuk:

Pentadbir E-mel,
Penyelaras ICT
Bahagian

- a. menghadkan jenis dan saiz fail lampiran bagi tujuan mengelakkan jangkitan virus dan serangan e-mel *bombing*;
- b. penghantaran dokumen rasmi hendaklah menggunakan e-mel rasmi jabatan sahaja;
- c. penggunaan e-mel JPA bagi tujuan peribadi adalah tidak dibenarkan;
- d. pentadbir e-mel perlu menetapkan had minimum kuota *mailbox* mengikut gred;
- e. pengemaskinian e-mel hendaklah dibuat sekiranya *mailbox* pengguna tidak aktif selama satu (1) bulan kecuali menerima pemakluman rasmi bagi mengesahkan pengguna *mailbox* masih aktif;
- f. penghantaran lampiran dalam format atau *extension* **.exe*, **.bat* dan **.com* tidak dibenarkan;



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

90 dari 128

- g. hanya warga JPA atau pengguna yang dibenarkan sahaja boleh dipertimbangkan untuk mendapat kemudahan e-mel rasmi jabatan;
- h. penyelaras ICT Bahagian perlu memaklumkan sebarang status pengguna (bertukar jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke JPA) di bahagian masing-masing bagi tujuan pengemaskinian e-mel yang terlibat;
- i. menggunakan kaedah inovatif dalam penghantaran fail bersaiz besar seperti menggunakan kaedah muat turun fail dengan memaklumkan lokasi *Universal Resource Location* (URL) atau kaedah pemampatan untuk mengurangkan saiz fail dengan memastikan ciri-ciri keselamatan dilaksanakan;
- j. e-mel rasmi yang dihantar atau diterima hendaklah disimpan dan diarkibkan mengikut panduan yang digariskan; dan
- k. menggunakan enkripsi bagi dokumen terperingkat yang dihantar secara elektronik.



PEROLEHAN, PEMBANGUNAN & PENYELENGGARAAN SISTEM

KAWALAN

Polisi Keselamatan Siber JPA Versi 1.1

10



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

91 dari 128

Kawalan 10: Perolehan, Pembangunan dan Penyelenggaraan Sistem

Objektif

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

K10/01 Kawalan Prosesan Aplikasi

	a. perolehan dan pembangunan, penambahbaikan serta penyelenggaraan sistem secara dalaman atau luaran hendaklah mengambil kira kawalan keselamatan bagi memastikan keselamatan sistem dan maklumat; b. ujian keselamatan hendaklah dijalankan ke atas sistem aplikasi untuk menyemak dan memastikan keselamatan sistem dan maklumat; dan c. sistem hendaklah diuji bagi memastikan sistem berkenaan memenuhi keperluan keselamatan sebelum digunakan dan dalam tempoh penyenggaraan.	ICTSO, Pentadbir Sistem
--	--	----------------------------

K010/01/01 Pengesahan Data Input

	Input data ke dalam aplikasi perlulah melalui proses pengesahan bagi memastikan data yang dimasukkan adalah tepat dan boleh dipercayai.	Pentadbir Sistem
--	---	------------------

K10/01/02 Kawalan Prosesan

	Mekanisme semasa pemprosesan data perlu diwujudkan bagi mengesan sebarang perubahan yang berlaku semasa proses dilaksanakan di dalam sistem.	Pentadbir Sistem
--	--	------------------



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

92 dari 128

K10/01/03 Pengesahan Data *Output*

Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.

Pentadbir Sistem
Aplikasi

K10/02 Keselamatan Fail Sistem

Fail sistem perlu dikawal dan dikendalikan dengan baik dan selamat.

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

Pentadbir Sistem



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

93 dari 128

K10/03 Keselamatan Dalam Proses Pembangunan dan Sokongan

K10/03/01 Peraturan Keselamatan Dalam Pembangunan Sistem

	Tatacara pembangunan perisian dan sistem yang mengambil kira aspek keselamatan maklumat hendaklah diwujudkan dan dilaksanakan di dalam organisasi.	Pengurus ICT
--	--	--------------

K10/03/02 Prosedur Perubahan

	Perubahan atau pengubahsuaian ke atas kitaran hayat pembangunan sistem, sistem pengoperasian dan aplikasi hendaklah dikawal, diuji, direkod dan disahkan sebelum digunakan mengikut SOP yang telah ditetapkan.	Pentadbir Sistem dan Pemilik Proses atau Sistem
--	--	---

K10/03/03 Semakan Teknikal Aplikasi Selepas Perubahan Platform

	Semakan dan pengujian terhadap aplikasi perlu dilaksanakan sekiranya berlaku perubahan terhadap platform pengoperasian bagi memastikan fungsi dan operasi sistem tidak terjejas. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan sistem aplikasi, integriti data dan kawalan akses disemak supaya operasi sistem tidak terjejas apabila perubahan platform dilaksanakan; dan b. Ujian penerimaan pengguna perlu dilaksanakan setelah perubahan platform selesai dilaksanakan.	Pentadbir Sistem
--	---	------------------

K10/03/04 Kawalan Terhadap Perubahan Kepada Perisian

	Mengawal perubahan dan/atau pindaan ke atas perisian dan aplikasi bagi memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja.	Pentadbir Sistem
--	---	------------------



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

94 dari 128

K10/03/05 Prinsip Kejuruteraan Sistem Yang Selamat

Prinsip kejuruteraan keselamatan sistem hendaklah dibangunkan, didokumenkan, dikaji dan diguna pakai ke atas semua pelaksanaan sistem maklumat.

Pentadbir Sistem,
Pembangun Sistem

K10/03/06 Persekitaran Pembangunan Sistem Yang Selamat

Persekitaran pembangunan sistem yang selamat perlu diwujudkan sepanjang kitar hayat pembangunan sistem.

Pentadbir Sistem

K10/03/07 Pembangunan Sistem Secara Luaran (Outsource)

Pembangunan perisian aplikasi secara *outsource* hendaklah mematuhi perkara-perkara berikut:

- setiap projek perlu dipantau oleh Pengurus ICT;
- kontrak perbekalan hendaklah memasukkan klausa kod sumber menjadi hak milik JPA;
- kod sumber yang diserahkan kepada JPA mesti bebas daripada sebarang ralat dan kerentanan;
- mengutamakan kepakaran teknologi tempatan;
- pembangunan aplikasi hendaklah dijalankan dalam persekitaran JPA;
- penggunaan *data masking/dummy data* semasa pembangunan dan pengujian;
- data ujian hendaklah dilupuskan secara kekal (secured delete) selepas projek disiapkan/tamat kontrak; dan

Pengurus ICT



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

95 dari 128

h. aktiviti sandaran penuh (full backup) ke atas keseluruhan sistem hendaklah berjaya dilakukan sebelum projek tamat.

K10/03/08 Ujian Keselamatan Sistem

Aktiviti pengujian keselamatan sistem hendaklah dilaksanakan atas sistem baharu, tambah baik, naik taraf dan versi baharu berdasarkan kriteria yang telah ditetapkan.

Pengurus ICT,
Pentadbir Sistem

K10/03/09 Pembocoran Maklumat

Sebarang peluang untuk membocorkan mesti dihalang.

ICTSO

K10/04 Data Ujian

Memastikan data yang digunakan untuk pengujian adalah dilindungi.

Pengurus ICT

K10/05 Kawalan Terhadap Keterdedahan Teknikal

Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut:

- a. memperoleh maklumat keterdedahan teknikal sistem yang digunakan;
- b. menilai tahap kerentanan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan
- c. mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.

ICTSO,
Pentadbir Sistem



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

96 dari 128

K10/06 Perkhidmatan E-dagang

Bertujuan untuk memastikan keselamatan perkhidmatan e-dagang dan penggunaannya.

- a. maklumat yang terlibat dalam e-dagang mesti dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan;
- b. maklumat yang terlibat menerusi transaksi dalam talian (online) mesti 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 mesti dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.

Pentadbir Sistem,
Pengguna

K10/07 Pembangunan Aplikasi Mudah Alih

Menerangkan perkara yang mesti dipatuhi dalam membangunkan aplikasi mudah alih bagi menjamin keselamatan aplikasi dan data.

Pentadbir Sistem

K10/07/01 Prosedur Integrasi Pembangunan Aplikasi Mudah Alih

Pembangunan aplikasi mudah alih yang melibatkan integrasi dengan sistem induk mesti menggunakan *Application Programming Interface* (API) atau lain-lain kaedah yang bersesuaian yang mengurangkan risiko ancaman keselamatan.

Pentadbir Sistem;
Pembangun Sistem



HUBUNGAN PEMBEKAL

KAWALAN

Polisi Keselamatan Siber JPA Versi 1.1

11



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

97 dari 128

Kawalan 11: Hubungan Pembekal

Objektif

Memastikan keselamatan aset ICT JPA yang diberi kebenaran capaian dilindungi.

K11/01 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal

- Perkara-perkara yang perlu dipatuhi adalah seperti berikut:
- 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.

Pengurus ICT,
Pembekal

K11/02 Pengurusan Penyampaian Perkhidmatan Pembekal

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

Pengurus ICT,
Pentadbir Sistem



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

98 dari 128

JPA hendaklah sentiasa memantau, mengkaji semula dan mengaudit penyampaian perkhidmatan pembekal. Perkara-perkara berikut hendaklah dipatuhi:

- a. pemantauan tahap prestasi perkhidmatan bagi mengesahkan pembekal mematuhi perjanjian perkhidmatan; dan
- b. laporan perkhidmatan yang dihasilkan oleh pembekal hendaklah dipantau dan status kemajuan dikemukakan kepada JPA.

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

Perkara-perkara yang perlu diambil kira adalah seperti berikut:

- a. perubahan dalam perjanjian dengan pembekal;
- b. perubahan yang dilakukan oleh JPA bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan
- c. perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, peralatan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.



RISIKO DAN PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

KAWALAN

Polisi Keselamatan Siber JPA Versi 1.1

12



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

99 dari 128

Kawalan 12: Risiko Dan Pengurusan Pengendalian Insiden Keselamatan

Objektif

Untuk memastikan semua insiden dikendalikan dengan konsisten, cepat, tepat dan berkesan termasuk saluran komunikasi keselamatan dan *security events* bagi memastikan sistem ICT JPA dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej JPA dan sistem penyampaian perkhidmatan.

K12/01 Mekanisme Pelaporan Insiden Keselamatan ICT

a. Pelaporan

Semua insiden keselamatan ICT yang berlaku mesti dilaporkan segera kepada JPACERT untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan bagi mengelakkan kerosakan bahan bukti tanpa melaksanakan tindakan secara sendirian. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan. Antara insiden keselamatan ICT yang perlu dilaporkan adalah:

- i. maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;
- ii. sistem maklumat digunakan tanpa kebenaran atau yang disyaki sedemikian;
- iii. kata laluan atau mekanisme kawalan akses yang hilang, dicuri, didedahkan atau yang disyaki sedemikian;

ICTSO, Pengguna,
JPACERT



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

100 dari 128

- iv. berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal berfungsi atau dicapai, dan komunikasi tersalah hantar; dan
- v. berlaku percubaan mencerooboh, penyelewengan dan insiden-insiden yang tidak dijangka yang boleh menjejaskan keselamatan ICT.

b. Pelaporan NACSA

- i. ICTSO melaporkan kepada NACSA apabila berlaku sebarang insiden keselamatan ICT sekiranya perlu; dan
- ii. Pasukan JPACERT dengan persetujuan ICTSO akan menghubungi NACSA untuk melaporkan atau mendapatkan bantuan apabila wujud potensi insiden atau berlaku sebarang insiden keselamatan ICT.

c. Tindakan Dalam Keadaan Berisiko Tinggi

Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak.

d. Pelaporan kepada JPACERT

Pentadbir sistem yang terlibat mesti melaporkan sebarang insiden yang melibatkan keselamatan ICT kepada JPACERT.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

101 dari 128

K012/02 Prosedur Pengurusan dan Pengendalian Insiden Keselamatan ICT

Pengurusan pengendalian insiden keselamatan ICT dilaksanakan oleh Pasukan JPACERT yang diketuai oleh ICTSO. Pengendalian ini dilaksanakan berpandukan prosedur pengurusan pelaporan dan pengendalian insiden keselamatan ICT JPA seperti di **Lampiran 2**.

ICTSO,
JPACERT

Pengendalian insiden keselamatan ICT perlu diuruskan dengan cepat, teratur dan berkesan, mengikut prosedur dengan mengambil kira langkah-langkah berikut:

- a. menerima laporan insiden daripada pengguna, pihak NACSA atau sumber lain;
- b. mengenal pasti semua jenis insiden keselamatan ICT;
- c. mematuhi Pelan Pemulihan Bencana (DRP) seperti yang telah digariskan dalam PKP;
- d. menyimpan jejak audit dan memelihara bahan bukti dan rekod;
- e. mengambil tindakan pengukuhan ke atas insiden;
- f. menyediakan tindakan pencegahan supaya insiden serupa tidak berulang; dan
- g. memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.



KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

KAWALAN

Polisi Keselamatan Siber JPA Versi 1.1

13



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

102 dari 128

Kawalan 13: Keselamatan Maklumat Bagi Pengurusan Kesenambungan Perkhidmatan

Objektif

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

K13/01 Pengurusan Kesenambungan Perkhidmatan

Pengurusan Kesenambungan Perkhidmatan (PKP) ialah mekanisme bagi mengurus dan memastikan kepentingan *stakeholder* sistem penyampaian perkhidmatan dilindungi dan imej JPA terpelihara. Ini dilakukan dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan JPA di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan.

Ketua Jabatan adalah bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT JPA.

Tiga (3) pasukan ditubuhkan di bawah PKP JPA iaitu Pasukan Tindak Balas Kecemasan (ERT), Pasukan Pemulihan Bencana (DRT) dan Pasukan Komunikasi Krisis (CCT) bagi melicinkan pelaksanaan PKP di JPA. Ahli ERT, DRT dan CCT adalah dilantik secara rasmi oleh pihak pengurusan JPA. Pelan PKP perlu dibangunkan dan mengandungi perkara-perkara berikut:

Pasukan PKP,
Pasukan Tindak Balas
Kecemasan (ERT),
Pasukan Pemulihan
Bencana (DRT) dan
Pasukan Komunikasi
Krisis (CCT)



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

103 dari 128

- a. senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
- b. senarai pengguna berserta nombor yang boleh dihubungi (faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan pegawai 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.

Salinan pelan PKP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan PKP hendaklah diuji sekurang-kurangnya sekali 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 tujuan dibangunkan.

Ujian pelan PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan pegawai yang terlibat



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

104 dari 128

mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.

JPA hendaklah memastikan salinan pelan PKP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

K13/01/01 Pelan Pemulihan Bencana

Pelan Pemulihan Bencana (DRP) merujuk kepada dokumen pelan yang menetapkan sumber, tindakan, tanggungjawab dan data yang diperlukan untuk mengurus proses pemulihan selepas berlaku gangguan terhadap perkhidmatan ICT JPA. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT dan perkara-perkara berikut perlu diberi perhatian:

- mengenal pasti semua tanggungjawab dan prosedur kecemasan dan pemulihan;
- melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;
- mendokumentasikan proses dan prosedur yang telah dipersetujui;
- mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT;

Pasukan PKP,
Pasukan Tindak Balas
Kecemasan (ERT),
Pasukan Pemulihan
Bencana (DRT) dan
Pasukan Komunikasi
Krisis (CCT)



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

105 dari 128

- e. mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;
- f. membuat *backup*; dan
- g. menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.

K13/02 Lewahan (Redundancy)

Semua sistem aplikasi dan peralatan yang kritikal hendaklah mempunyai kemudahan lewahan dan diuji (failover test) keberkesanannya mengikut keperluan dan kesesuaian semasa.

Pengurus ICT,
Pentadbir Sistem



PEMATUHAN

KAWALAN

Polisi Keselamatan Siber JPA Versi 1.1

14



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

106 dari 128

Kawalan 14: Pematuhan

Objektif

Bagi mengelakkan pelanggaran peraturan berkanun undang-undang, kontrak dan PKS JPA.

K14/01 Pematuhan Dasar

Setiap pengguna di JPA hendaklah membaca, memahami dan mematuhi PKS JPA dan undang-undang atau peraturan-peraturan lain yang berkaitan.

Pengguna

Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua warga di JPA adalah seperti di **Lampiran 5** tertakluk kepada kesesuaian JPA.

Perkara yang perlu dipatuhi adalah seperti berikut:

- semua perlembagaan, undang-undang, peraturan, perjanjian yang dimeterai dan lain-lain perkara yang relevan kepada keselamatan sistem maklumat dan organisasi hendaklah dikenal pasti, di dokumentasikan dan dikemas kini;
- peraturan yang sesuai dilaksanakan untuk pematuhan ke atas perlembagaan, undang-undang dan keperluan perjanjian mengenai penggunaan material yang tertakluk kepada hak milik harta intelek;
- rekod penting hendaklah dilindungi daripada hilang, rosak atau dipalsukan selaras dengan keperluan undang-undang, peraturan dan keperluan perjanjian JPA;



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

107 dari 128

- d. perlindungan ke atas data dan maklumat privasi hendaklah mematuhi perundangan, peraturan dan terma perjanjian jika perlu; dan
- e. penggunaan kriptografi perlu dikawal selia selaras dengan perjanjian, perundangan dan peraturan yang berkuat kuasa.

K14/02 Pematuhan kepada Dasar, Peraturan dan Penilaian Teknikal Keselamatan

ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal.

ICTSO

Sistem ICT maklumat perlu melalui penilaian pemeriksaan secara berkala bagi mematuhi piawaian pelaksanaan keselamatan.

Sebarang penilaian pematuhan teknikal seperti aktiviti *Security Posture Assessment* (SPA) mestilah dijalankan oleh pihak yang kompeten dan dibenarkan oleh JPA.

K14/03 Pematuhan Keperluan Audit

Pematuhan kepada keperluan audit perlu bagi meminimumkan risiko ancaman dan memaksimumkan keberkesanan dalam pengurusan keselamatan JPA (dalam proses audit sistem maklumat).

ICTSO

Keperluan pelaksanaan audit dan sebarang aktiviti penilaian dan pemeriksaan ke atas sistem ICT perlu dirancang dan dipersetujui ICTSO bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

108 dari 128

Capaian ke atas peralatan audit sistem maklumat perlu dikawal dan diselia bagi mengelakkan berlaku penyalahgunaan.

K14/04 Pelanggaran Perundangan

Pelanggaran dasar ini boleh diambil tindakan undang-undang dan tatatertib di bawah Akta Rahsia Rasmi 1972 dan Perintah-perintah Am Bab "D" - Peraturan-peraturan Pegawai Awam (Kelakuan Dan Tatatertib).

Pengguna



GLOSARI



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

109 dari 128

Glosari

<i>Active Directory (AD)</i>	Teknologi <i>Microsoft</i> yang digunakan untuk mengurus komputer dan peralatan lain dalam rangkaian.
Antivirus	Perisian yang mengimbas virus pada media storan, seperti cakera keras (hard disk) dan disket (diskette) untuk sebarang kemungkinan adanya virus.
Aplikasi	Perisian komputer atau program yang khusus digunakan untuk peranti mudah alih.
Aset Alih	Aset alih bermaksud aset yang boleh dipindahkan dari suatu tempat ke suatu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
Aset ICT	Aset ICT terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia yang mempunyai nilai.
<i>Backup</i>	Proses penduaan sesuatu dokumen atau maklumat.
<i>Bandwidth</i>	Jalur lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh: di antara cakera keras dan PC utama) dalam jangka masa yang ditetapkan.
Bilik khas	Bilik yang selamat dan terkawal.
BYOD	<i>Bring Your Own Device.</i>



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

110 dari 128

CCTV

Closed-circuit television

Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang dalam premis pejabat bagi tujuan membantu pemantauan fizikal.

CERT Agensi

Computer Emergency Response Team

Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.

CIO

Chief Information Officer

Ketua Pegawai Maklumat yang bertanggungjawabkan terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.

Clear Desk dan Clear Screen

Tidak meninggalkan dokumen data dan maklumat terperingkat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.

Data-at-rest

Data-at-rest (data-dalam-simpanan)

Data yang tidak aktif yang disimpan secara fizikal dalam bentuk digital (contohnya pangkalan data, gudang data, hamparan, arkib dan sebagainya).

Data-in-motion

Data-in-motion (data-dalam-pergerakan)

Data-dalam-pergerakan atau data transit maklumat digital yang sedang dalam proses pergerakan di dalam atau antara sistem komputer.

Data-in-use

Data-in-use (data-dalam-penggunaan)

Data yang digunakan ialah data yang sedang diperbaharui, diproses, dihapus, diakses atau dibaca oleh sistem. Jenis data ini tidak disimpan secara pasif, tetapi bergerak aktif melalui infrastruktur IT



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

111 dari 128

Data masking

Data masking ialah kaedah penyembunyian data asli yang digunakan untuk tujuan pengujian dan latihan.

Defence-in-depth

Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.

Denial of service

Halangan pemberian perkhidmatan.

Downloading

Aktiviti muat-turun sesuatu perisian.

DRC

Disaster Recovery Centre
Pusat Pemulihan Bencana

DRP

Disaster Recovery Plan
Pelan Pemulihan Bencana

Dummy data

Dummy data ialah data yang tidak bermakna yang digunakan untuk tujuan pengujian dan latihan.

Encryption

Enkripsi atau penyulitan. Proses enkripsi data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.

Firewall

Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk peralatan atau perisian atau kombinasi kedua-duanya.

Forgery

Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft/espionage), penipuan (hoaxes).



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

112 dari 128

Hard disk

Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.

ICT

Information and Communication Technology

ICTSO

ICT Security Officer

Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.

Insiden Keselamatan

Musibah (adverse event) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.

INTAN

Institut Tadbiran Awam Negara.

ISDN

Integrated Services Digital Networks

Menggunakan isyarat digital pada talian telefon analog yang sedia ada.

Internet

Sistem rangkaian seluruh dunia, di mana pengguna pada mana-mana komputer boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.

Internet Gateway

Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.

Intranet

Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.

Intrusion Detection System (IDS)

Sistem Pengesan Pencerobohan

Perisian atau peralatan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpanduan



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

113 dari 128

Intrusion Prevention System (IPS)

jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.

Sistem Pencegah Pencerobohan

Peralatan keselamatan yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Berperanan bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Sebagai contoh, *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.

ISMS JPA

Information Security Management System

Organisasi JPA merangkumi bahagian-bahagian seperti berikut:

1. Bahagian Penyelidikan, Perancangan dan Dasar (BPPD)
2. Bahagian Pembangunan Organisasi (BPO);
3. Bahagian Perkhidmatan (BK);
4. Bahagian Saraan (BS);
5. Bahagian Pembangunan Modal Insan (BMI);
6. Bahagian Khidmat Pengurusan (BKP);
7. Bahagian Pasca Perkhidmatan (BP);
8. Bahagian Pembangunan dan Pengurusan Maklumat Strategik (BPMS);
9. Bahagian Pengurusan Psikologi (BPPs); dan
10. Institut Tadbiran Awam Negara (INTAN)

Keadaan Berisiko Tinggi

Dalam situasi yang mudah mendapat ancaman keselamatan ICT yang boleh menjejaskan kelancaran operasi dan sistem ICT JPA.

Kriptografi

Kaedah untuk menukar data dan maklumat biasa (piawaian format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.

KPKK

Ketua Pegawai Keselamatan Kerajaan.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

114 dari 128

LAN

Local Area Network

Rangkaian Kawasan Setempat yang menghubungkan komputer.

Lightning arrestor

Alat yang digunakan untuk mencegah daripada ancaman kilat.

Lock

Mengunci komputer.

Log out

Log-out komputer

Keluar daripada sesuatu sistem atau aplikasi komputer.

Malicious Code

Merupakan perisian hasad atau jahat yang memasuki sistem komputer dan menyebabkan risiko keselamatan seperti kerosakan komputer, gangguan capaian Internet dan sebagainya tanpa disedari oleh pengguna.

MODEM

MODulator DEModulator

Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.

Mobile Code

Mobile code merupakan perisian yang boleh dipindahkan antara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh Java Applet, ActiveX dan sebagainya pada pelayar Internet.

NACSA

National Cyber Security Agency

Agensi Keselamatan Siber Negara

Outsource

Maklumat yang diproses dan diperoleh di luar daripada sesuatu organisasi atau struktur kerja.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

115 dari 128

Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan daripada segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
Pegawai Keselamatan	Memastikan keselamatan perlindungan di jabatan terjamin sepanjang masa.
Pembangun Sistem	Individu atau kumpulan teknikal atau pihak luaran yang bertanggungjawab dalam membangunkan sistem aplikasi berdasarkan spesifikasi keperluan sistem yang ditetapkan oleh pemohon/pemilik proses.
Pengguna	Pengguna terdiri daripada warga JPA dan pihak luaran yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT JPA.
Pengurus ICT	Pegawai yang mengetuai organisasi ICT di Jabatan/Bahagian/Unit berkaitan ICT.
Penyelaras ICT Bahagian	Pegawai Penyelaras ICT merupakan pegawai yang mahir dan berkelayakan mengenai bidang ICT dan dilantik oleh Pengarah Bahagian. Peranan dan tanggungjawab:- - Perolehan Aset; - Penerimaan Aset; - Pendaftaran Aset; - Penggunaan, Penyimpanan dan Pemeriksaan; - Penyelenggaraan; - Pelupusan; dan - Penyelenggaraan Sistem Aplikasi Teras.
Peralatan Sokongan ICT	Peralatan yang menyokong penggunaan peralatan ICT bagi memastikan kelancaran ICT contohnya projektor, layar, kabel, speaker dan mikrofon.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

116 dari 128

Peripheral

Perisian

Aset yang digunakan untuk menyokong pemprosesan maklumat.

Program atau atur cara komputer yang dapat digunakan dengan sistem komputer tertentu.

Perisian Aplikasi

Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.

Pihak Luaran

Pihak luaran terdiri daripada pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan atau pelawat yang mengunjungi JPA atas urusan rasmi.

PKI

Public-Key Infrastructure
Infrastruktur Kunci Awam

PKP

Pengurusan Kesenambungan Perkhidmatan

PSM

Pengurusan Sumber Manusia

Pusat Data JPA

Pusat Data JPA merangkumi dua (2) pengurusan pusat data utama iaitu Pusat Data JPA (BPMS) dan Pusat Data INTAN.

Rahsia

Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing.

Rahsia Besar

Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

117 dari 128

Restoration

Pemulihan ke atas data.

Router

Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.

Screen saver

Imej yang akan diaktifkan pada komputer setelah ia tidak digunakan dalam jangka masa tertentu.

Server

Pelayan

Sistem

Kumpulan dari elemen-elemen yang berinteraksi untuk mencapai suatu tujuan tertentu.

Sulit

Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.

Switch

Alat yang boleh menapis (filter) dan memajukan (forward) isyarat paket data antara segmen rangkaian LAN.

Terhad

Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan.

Threat

Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

118 dari 128

Uninterruptible Power Supply (UPS)

Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan daripada sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.

Video conference

Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.

Video streaming

Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.

Virus

Atur cara yang bertujuan merosakkan data atau sistem aplikasi.

WAN

Wide Area Network

Rangkaian yang merangkumi kawasan yang luas.

Wireless LAN

Jaringan komputer yang terhubung tanpa melalui kabel.

Worm

Sejenis virus yang boleh beraplikasi dan membiak dengan sendiri. Ia biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.



SENARAI LAMPIRAN

Polisi Keselamatan Siber JPA Versi 1.1



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

119 dari 128

LAMPIRAN 1

SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER JPA

Nama (Huruf Besar) :
No. Kad Pengenalan :
Jawatan :
Bahagian (JPA) :
Organisasi (selain warga JPA):
No. Kontrak (jika berkaitan) :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :

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

Tandatangan :

Tarikh :



POLISI KESELAMATAN SIBER JPA

Versi:

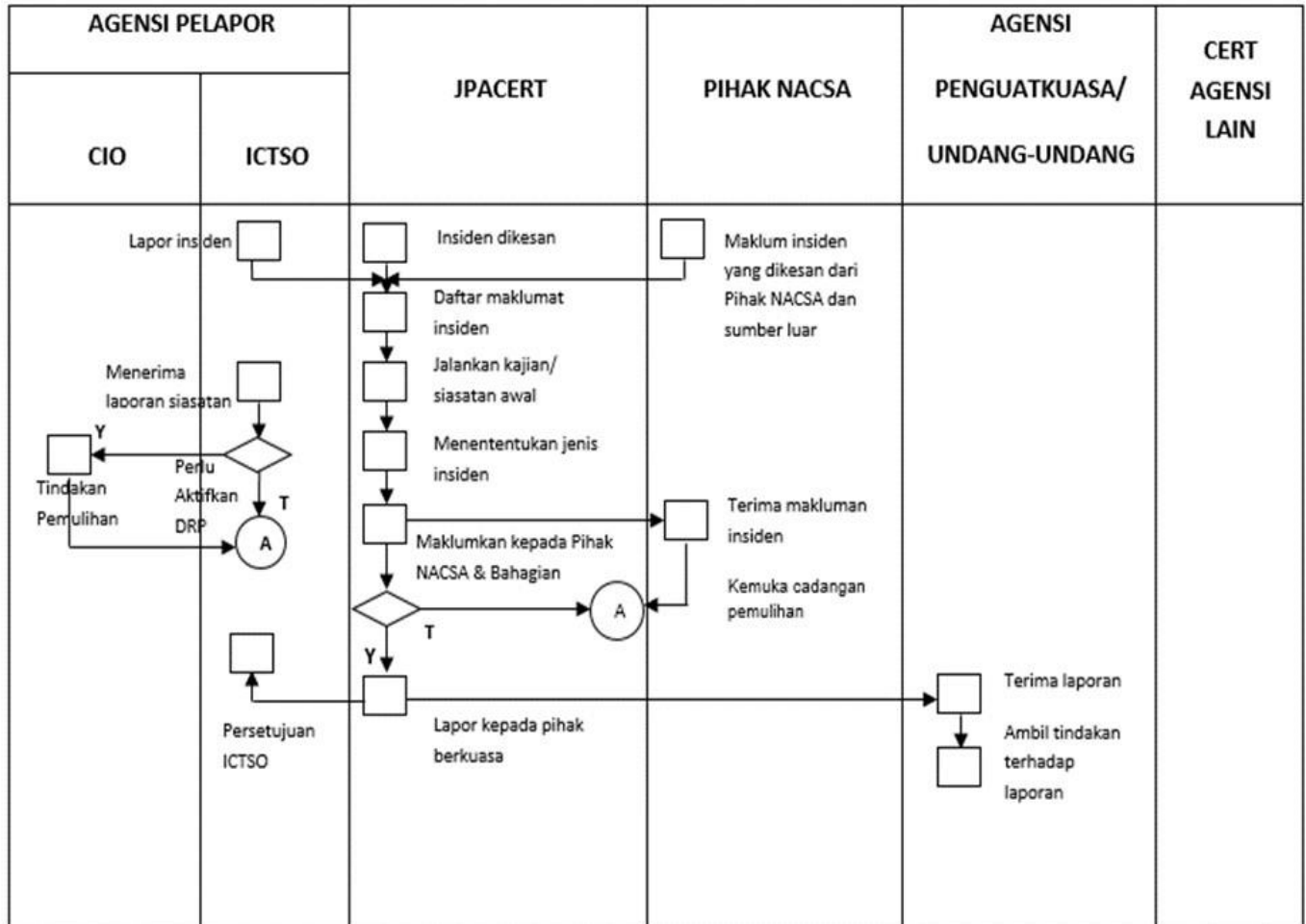
1.1

Muka Surat:

120 dari 128

LAMPIRAN 2

Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT JPA





POLISI KESELAMATAN SIBER JPA

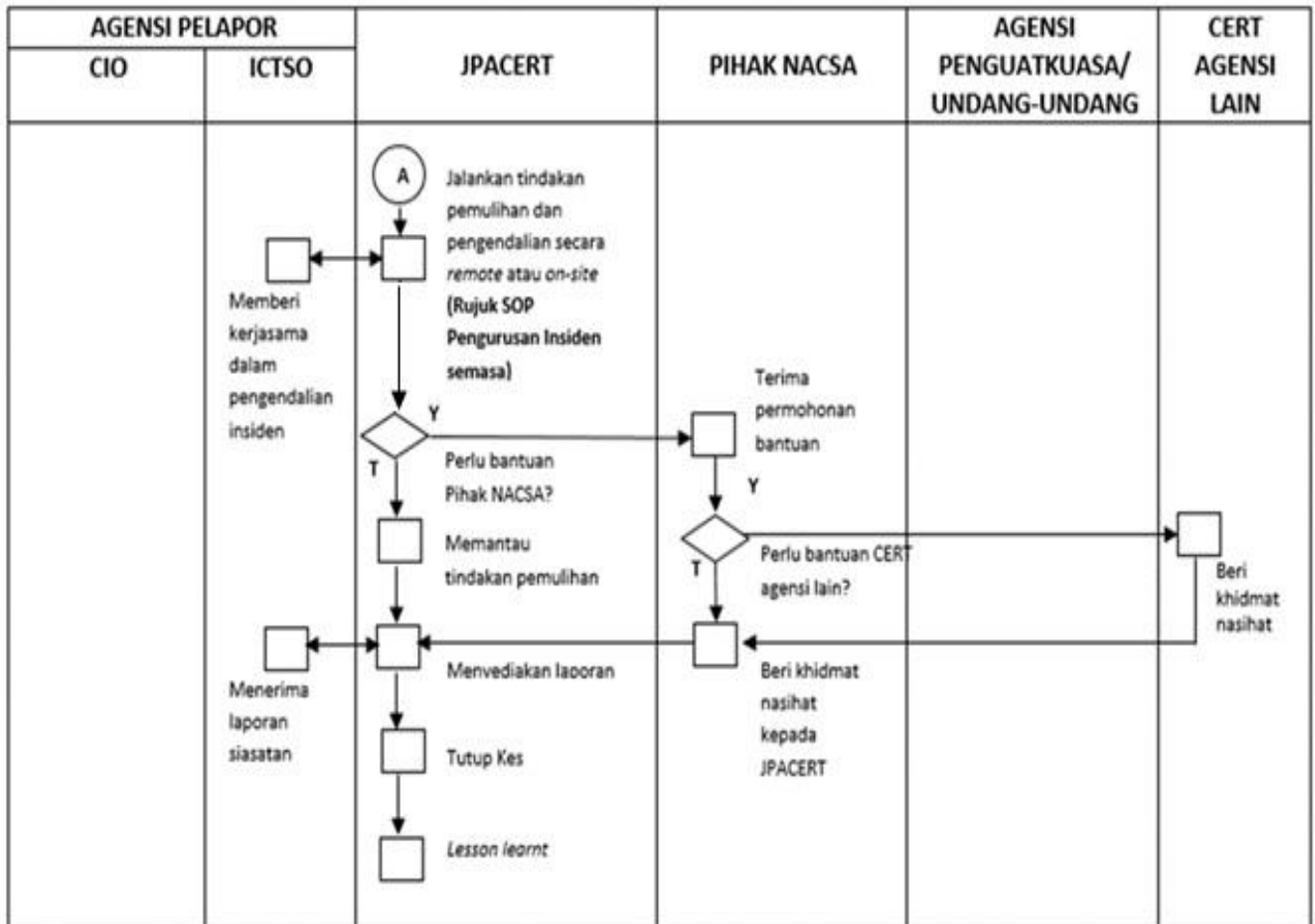
Versi:

1.1

Muka Surat:

121 dari 128

Rajah 2: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT JPA (sambungan)





POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

122 dari 128

LAMPIRAN 3

PERMOHONAN KEBENARAN UNTUK MENGGUNAKAN KEMUDAHAN INTERNET PERIBADI BAGI TUJUAN SAMBUNGAN KE INTERNET

Nama (Huruf Besar) :
No. Kad Pengenalan :
Jawatan :
Bahagian (JPA) :
Organisasi (selain warga JPA):
No. Kontrak (jika berkaitan) :

Saya dengan ini memohon kebenaran daripada Pengurus ICT JPA untuk menggunakan modem peribadi bagi tujuan seperti berikut :

Saya juga sedar bahawa saya terikat dengan peraturan-peraturan seperti yang telah ditetapkan di dalam dokumen Polisi Keselamatan Siber (PKS) JPA. Dan jika saya ingkar kepada peruntukan-peruntukan tersebut, maka tindakan sewajarnya boleh diambil ke atas diri saya. Kebenaran ini juga tertakluk kepada empat (4) syarat berikut;

- i. penggunaan ini adalah untuk urusan rasmi sahaja
- ii. memastikan perisian antivirus sentiasa aktif (activated) dan dikemas kini di samping turut melakukan imbasan ke atas media storan yang digunakan
- iii. memasang dan menggunakan hanya perisian yang tulen
- iv. tidak menyambungkan *notebook* kepada rangkaian dalaman Jabatan (wired/wireless) dan kemudahan Internet peribadi secara serentak.

Saya mengesahkan bahawa penggunaan Internet peribadi telah mengikut peraturan seperti di atas. Maklumat kemudahan yang akan digunakan adalah seperti berikut:

Tandatangan :

Tarikh :



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

123 dari 128

Pengesahan Penyelia ICT

.....

(Nama Penyelia ICT)

b.p. Ketua Pengarah Perkhidmatan Awam

Tarikh:

Kelulusan Pengurus ICT

.....

(Nama Pengurus ICT)

b.p. Ketua Pengarah Perkhidmatan Awam

Tarikh:



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

124 dari 128

LAMPIRAN 4

DECLARATION TO BE SIGNED BY CONTRACTORS ENGAGED ON GOVERNMENT PROJECTS IN RESPECTS OF THE OFFICIAL SECRETS ACT 1972

I hereby acknowledge that my attention has been drawn to the provisions of the Official Secrets Act 1972 (Act 88), as amended, and that fully understand the implications contained thereof. In particular I understand that to communicate to unauthorised person, to use or having in possession without authorisation any classified materials, and failure to take reasonable care of classified materials, I shall be guilty of an offence under this Act and punishable with imprisonment for life.

I understand that all official information acquired by me in the service of His Majesty the Yang di-Pertuan Agong or any Government in the Federation, is the property of the Government and is not to be divulged, published, or communicated, whether orally or in writing, to any other person in any form, except in the course of my official duties, whether during or after my service with His Majesty the Yang di-Pertuan Agong or Government in the Federation without the previous sanction in writing of the relevant authority. I undertake to sign a further declaration to this effect on completion of the Government Project.

Signature :

Name In Capital Letter :

Identification Card No :

Position :

Department :

Date :



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

125 dari 128

PERAKUAN UNTUK DITANDATANGANI OLEH KONTRAKTOR YANG TERLIBAT DENGAN PROJEK KERAJAAN MENURUT AKTA RAHSIA RASMI 1972

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu rahsia atau apa-apa tingkah laku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi suatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

Saya faham bahawa segala maklumat rasmi yang saya peroleh dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan, atau menyampaikan, sama ada secara lisan atau dengan bertulis, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapat kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani suatu akuan selanjutnya bagi maksud ini apabila tamat projek Kerajaan.

Tandatangan :

Nama dengan Huruf Besar :

No Kad Pengenalan :

Jawatan :

Jabatan :

Tarikh :



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

126 dari 128

LAMPIRAN 5

BIL.

SENARAI PERUNDANGAN DAN PERATURAN

1.	Akta Tandatangan Digital 1997;
2.	Akta Rahsia Rasmi 1972;
3.	Akta Jenayah Komputer 1997;
4.	Akta Hak cipta (Pindaan) Tahun 1997;
5.	Akta Komunikasi dan Multimedia 1998;
6.	Akta 709 – Akta Perlindungan Data Peribadi 2010;
7.	Akta 658 – Akta Perdagangan Elektronik 2006;
8.	Akta 629 – Akta Arkib Negara 2003;
9.	Akta 606 – Akta Cakera Optik 2000;
10.	Akta 298 – Kawasan Larangan Tempat Larangan 1959;
11.	Akta 56 – Akta Keterangan 1950;
12.	Arahan Keselamatan;
13.	Arahan Perbendaharaan;
14.	Arahan Teknologi Maklumat 2007
15.	Arahan 20 (Semakan Semula) – Dasar dan Mekanisme Pengurusan Bencana Negara;
16.	Arahan 24 – Dasar dan Mekanisme Pengurusan Krisis Siber Negara;
17.	Dasar Pengurusan Rekod dan Arkib Elektronik
18.	Etika Penggunaan E-mel dan Internet JPA;
19.	Garis Panduan Penerapan Etika Penggunaan Media Sosial Dalam Sektor Awam (MAMPU);
20.	Garis Panduan Perolehan ICT Kerajaan Kementerian Kewangan Malaysia. Cabutan Pekeliling Perbendaharaan Malaysia PK 2.2/2013;
21.	Garis Panduan IT Outsourcing Agensi-Agensi Sektor Awam 04/2006;
22.	Garis Panduan Pengurusan Rekod;
23.	Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi;
24.	Guideline to Determine Information Security Professionals Requirement for the CNII Agencies /Organisations;
25.	National Cyber Security Policy (NCSP);
26.	Panduan Pelaksanaan Audit ISMS Sektor Awam;



POLISI KESELAMATAN SIBER JPA

Versi:

1.1

Muka Surat:

127 dari 128

27. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan";
28. Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 bertajuk "Pengurusan Laman Web Agensi Sektor Awam";
29. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)";
30. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan";
31. Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 bertajuk "Panduan Pengurusan Pejabat bertarikh 30 April 2007";
32. Pekeliling Transformasi Pentadbiran Awam Bilangan 3 Tahun 2017: Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan;
33. Pekeliling Am Bilangan 1 Tahun 2015 – Pelaksanaan Data Terbuka Sektor Awam;
34. Pekeliling Perbendaharaan Malaysia PK 2/2013 – Kaedah Perolehan Kerajaan;
35. Perintah-Perintah Am;
36. Pelan Pengurusan Pemulihan Bencana JPA;
37. PK3.2 - Manual Perolehan Perkhidmatan Perunding Edisi 2011 (Pindaan Kedua);
38. Polisi Keselamatan Siber MAMPU
39. Prosedur Pengurusan Pelaporan Dan Pengendalian Insiden Keselamatan ICT JPA;
40. 1Pekeliling Perbendaharaan AM 2 Tahun 2018: Tatacara Pengurusan Aset Alih Kerajaan;
41. Rancangan Malaysia Ke-11;
42. Surat Arahan KPPA Tindakan Ke Atas Penjawat Awam Yang Mendedahkan/Membocorkan Dokumen/Maklumat Terperingkat Kerajaan bertarikh 28 Januari 2015;
43. Surat Arahan MAMPU.702-1/1/7 Jld. 3 (48) bertarikh 23 Mac 2009 bertajuk "Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-agensi Kerajaan";
44. Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 bertajuk "Penggunaan Media Jaringan Sosial di Sektor Awam";
45. Surat Arahan Ketua Pengarah MAMPU Pelaksanaan dan Penggunaan Aplikasi Digital Document Management System (DDMS) Sektor Awam yang bertarikh 26 Januari 2015;
46. Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat yang bertarikh 24 November 2010;



POLISI KESELAMATAN SIBER JPA

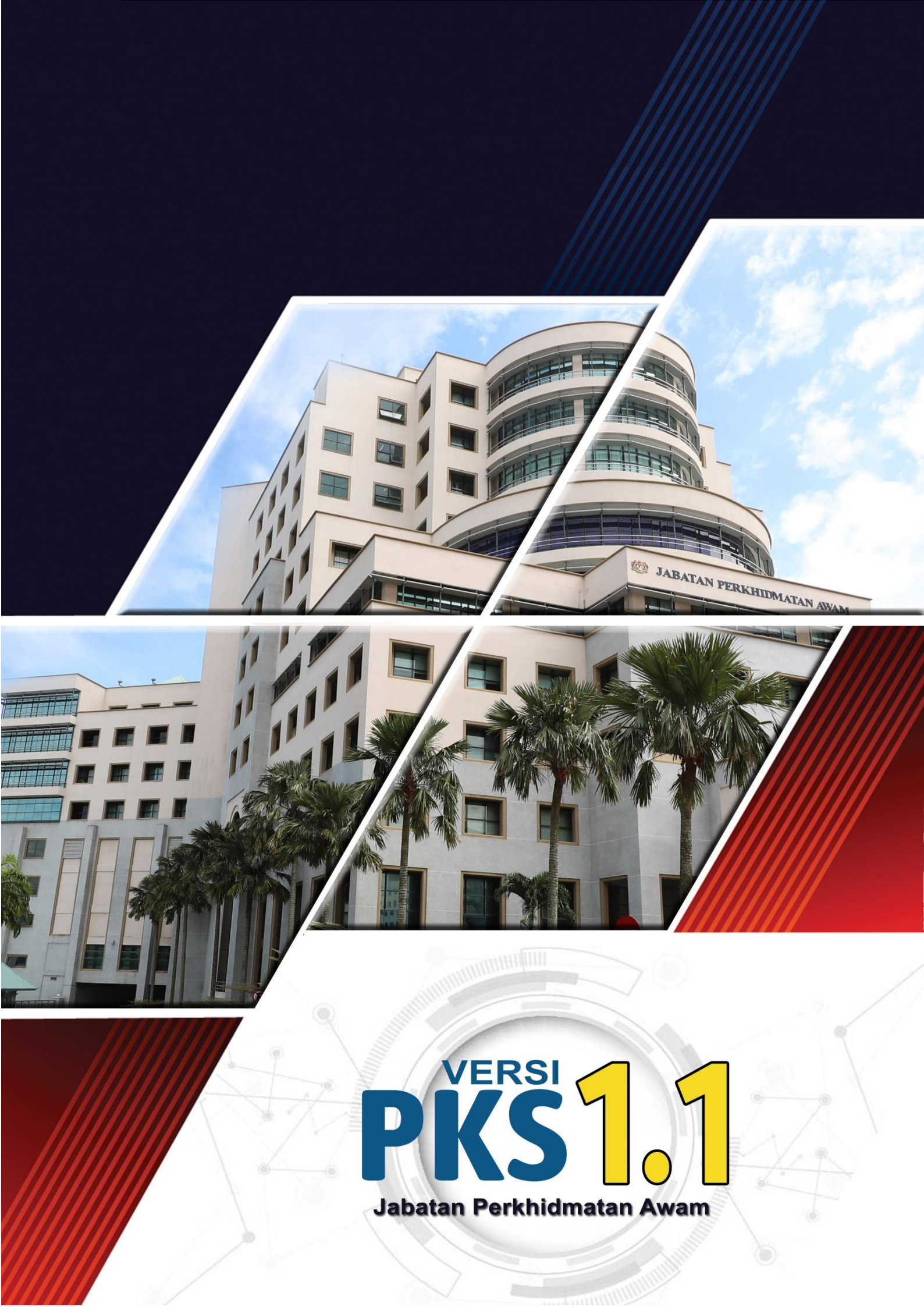
Versi:

1.1

Muka Surat:

128 dari 128

47. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesenambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010;
48. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
49. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
50. 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;
51. Surat Akujanji;
52. Surat Pekeliling Am Bilangan 3 Tahun 2015 bertajuk “Garis Panduan Permohonan Kelulusan Teknikal Dan Pemantauan Projek ICT Agensi Sektor Awam”;
53. Surat Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2015 bertajuk “Panduan Pelaksanaan Program Turun Padang Sektor Awam”;
54. Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk “Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam”;
55. Surat Pekeliling Am Bilangan 4 Tahun 2006 bertajuk “Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam”;
56. Surat Pekeliling Perbendaharaan – Garis Panduan Mengenai Pengurusan Perolehan *Information Telecommunication Technology* ICT Kerajaan SPP 3/2013;
57. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam;
58. Surat Pekeliling Am Bilangan 2/1987 – Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987);
59. Surat Pekeliling Am Bilangan 4 Tahun 2006 Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT) Sektor Awam Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) versi 1.0 April 2016;



VERSI
PKS 1.1
Jabatan Perkhidmatan Awam