



APPLICATION INFORMATION NETWORK



OPERATIONAL



ENCRYPTION



ACCESS CONTROL



END-USER
EDUCATION



DISASTER
RECOVERY

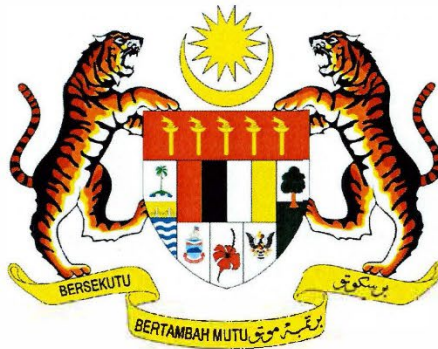


JABATAN KETUA PENGARAH TANAH
DAN GALIAN PERSEKUTUAN

POLISI KESELAMATAN SIBER

VERSI 2.0





**JABATAN KETUA PENGARAH TANAH DAN GALIAN
PERSEKUTUAN
KEMENTERIAN SUMBER ASLI DAN KELESTARIAN ALAM**

POLISI KESELAMATAN SIBER

JKPTG-ISMS-P1-001

ISO/IEC 27001:2022

Disediakan Oleh:  Nama: FATIMAH SHAM AMIR Jawatan: PENOLONG PENGARAH (PSI) Tarikh: 1 Oktober 2025	Disemak Oleh:  Nama: MUHAMMAD HEEZA BIN HASSAN Jawatan: Pengarah Pengurusan ICT Pentadbiran Tanah Jabatan Ketua Pengarah Tanah dan Galian Persekutuan Tarikh: 2 Oktober 2025	Diluluskan Oleh:  Nama: MUHAMMAD ROSLI BIN MUHAMMAD JA'APAR Jawatan: TIMBALAN KETUA PENGARAH (SKPP) Tarikh: 2 Oktober 2025
--	--	---



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

A. REKOD PINDAAN DOKUMEN

TARIKH	NO. KELUARAN/ PINDAAN	BAB / MUKA SURAT	KETERANGAN PINDAAN
13 Ogos 2024	1.0	Keseluruhan	Versi Awalan
2 Oktober 2025	2.0	Bab 1.3 Bab 2.1 Bab 6 Bab 11.3	Bab Penyelenggaraan Polisi Organisasi Keselamatan Maklumat Pencegahan Kebocoran Data (DLP) Keselamatan maklumat dalam pengurusan projek.



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

B. KANDUNGAN

SEJARAH DOKUMEN POLISI KESELAMATAN SIBER	9
PENGENALAN.....	10
OBJEKTIF	10
PENYATAAN POLISI.....	11
SKOP.....	12
PRINSIP-PRINSIP	14
SINGKATAN DAN TAKRIFAN.....	18
BAB 1: PELAKSANAAN POLISI.....	20
1.1 Pelaksanaan Polisi Keselamatan Siber JKPTG	20
1.2 Pemakaian Polisi.....	20
1.3 Penyelenggaraan Polisi.....	20
BAB 2: ORGANISASI KESELAMATAN	21
2.1 Organisasi Keselamatan Maklumat.....	21
2.1.1 Peranan dan tanggungjawab Ketua Jabatan	21
2.1.2 Peranan dan tanggungjawab Ketua Pegawai Digital (CDO).....	22
2.1.3 Peranan dan tanggungjawab Pegawai Keselamatan ICT (ICTSO)	22
2.1.4 Peranan dan tanggungjawab Pengurus ICT	23
2.1.5 Peranan dan tanggungjawab Pentadbir Sistem ICT	23
2.1.6 Peranan dan tanggungjawab Pentadbir Rangkaian dan Keselamatan ..	24
2.1.7 Peranan dan tanggungjawab Pentadbir Laman Web.....	25
2.1.8 Peranan dan tanggungjawab Pentadbir Pangkalan Data.....	25
2.1.9 Peranan dan tanggungjawab Pentadbir Pusat Data	26
2.1.10 Peranan dan tanggungjawab Pentadbir Sistem Aplikasi.....	27
2.1.11 Peranan dan tanggungjawab Pentadbir E-mel.....	28
2.1.12 Peranan dan tanggungjawab Pegawai Aset ICT.....	28
2.1.13 Peranan dan tanggungjawab Pengguna.....	30
2.2 Jawatankuasa Pemandu ICT (JPICT)	30
2.3 Jawatankuasa Keselamatan dan Operasi ICT (JKOICT)	30



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

2.4	Juruaudit.....	31
2.5	Penasihat Undang-undang.....	31
2.6	Pengurus Sumber Manusia.....	32
2.7	Pihak Ketiga	32
2.8	Peranti mudah alih dan <i>teleworking</i>	32
BAB 3:	KESELAMATAN SUMBER MANUSIA	34
3.1	Sebelum Dalam Perkhidmatan.....	34
3.2	Semasa Dalam Perkhidmatan.....	35
3.3	Bertukar/ Tamat Perkhidmatan/ Cuti Belajar	36
BAB 4:	PENGURUSAN ASET	38
4.1	Tanggungjawab Terhadap Aset	38
4.1.1	Inventori dan Pemilikan Aset ICT.....	38
4.1.2	Peralatan Mudah Alih dan Kerja Jarak Jauh.....	40
4.1.3	Peminjaman dan Pemulangan Aset ICT	40
4.2	Pengelasan, Pelabelan dan Pengendalian Maklumat	42
4.2.1	Pengelasan Maklumat	42
4.2.2	Pelabelan dan Pengendalian Maklumat.....	42
4.3	Pengendalian Media Penyimpanan Maklumat	43
BAB 5:	PENGURUSAN KAWALAN CAPAIAN.....	45
5.1	Keperluan Kawalan Capaian	45
5.2	Kawalan Capaian Rangkaian	46
5.3	Pengurusan Capaian Pengguna	46
5.4	Kawalan Capaian Sistem dan Aplikasi	48
5.5	Pengurusan Kata Laluan	50
5.6	Pengurusan Kata Laluan Super Administrator	51
5.7	Tanggungjawab Pengguna.....	51
BAB 6:	KRIPTOGRAFI	55
6.1	Kriptografi.....	55
6.2	<i>Data Masking</i>	56
6.3	Pencegahan Kebocoran Data (DLP).....	57
BAB 7:	KESELAMATAN FIZIKAL DAN PERSEKITARAN	58



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

7.1 Keselamatan Persekitaran	58
7.1.1 Keselamatan Fizikal.....	58
7.1.2 Kawalan Masuk Fizikal	60
7.1.3 Kawasan Larangan	60
7.1.4 Pemantauan Keselamatan Fizikal	62
7.2 Keselamatan Peralatan ICT dan Maklumat.....	62
7.2.1 Peralatan ICT.....	62
7.2.2 Media Storan	65
7.2.3 Media Tandatangan Digital.....	66
7.2.4 Media Perisian dan Aplikasi.....	67
7.2.5 Penyelenggaraan Peralatan ICT.....	67
7.2.6 Pinjaman Peralatan ICT.....	68
7.2.7 Peralatan ICT di Luar Premis Jabatan.....	69
7.2.8 Pelupusan Peralatan Aset ICT.....	70
7.2.9 Clear Desk dan Clear Screen	70
7.2.10 Perkhidmatan Awan (<i>Cloud Services</i>)	71
7.2.11 Penghapusan Maklumat	72
7.3 Keselamatan Persekitaran	73
7.3.1 Kawalan Persekitaran.....	73
7.3.2 Bekalan Kuasa.....	74
7.3.3 Kabel Peralatan ICT.....	75
7.3.4 Prosedur Kecemasan	76
7.4 Keselamatan Dokumen	76
7.4.1 Dokumen	76
BAB 8: KESELAMATAN OPERASI	78
8.1 Prosedur dan Tanggungjawab Operasi.....	78
8.1.1 Pengendalian Prosedur Operasi.....	78
8.1.2 Pengurusan Perubahan	79
8.1.3 Pengurusan Kapasiti.....	79
8.1.4 Pengurusan Konfigurasi.....	80
8.1.5 Pengasingan Kemudahan Pembangunan, Ujian dan Operasi.....	80



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

8.2 Perlindungan daripada <i>Malware</i>	81
8.3 <i>Backup</i>	82
8.4 Log dan Pemantauan	83
8.5 Kawalan Pengoperasian Perisian.....	85
8.6 Pengurusan Kerentanan Teknikal	86
8.7 Pemakluman Audit	86
BAB 9: KESELAMATAN KOMUNIKASI	87
9.1 Pengurusan Keselamatan Rangkaian	87
9.1.1 Kawalan Infrastruktur Rangkaian.....	87
9.1.2 Keselamatan Perkhidmatan Rangkaian.....	88
9.1.3 <i>Web Filtering</i>	89
9.1.4 Pengasingan Rangkaian.....	89
9.2 Pemindahan Maklumat.....	90
9.2.1 Prosedur Pemindahan Maklumat.....	90
9.2.2 Perjanjian Pemindahan dan Kerahsiaan Maklumat	91
9.2.3 Pengurusan Mesej Elektronik	92
BAB 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	93
10.1 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat	93
10.1.1 Perlindungan Perkhidmatan Aplikasi yang menggunakan Rangkaian Awam.....	94
10.1.2 Melindungi Transaksi Perkhidmatan Atas Talian	94
10.2 Keselamatan Dalam Proses Pembangunan dan Sokongan.....	95
10.2.1 Polisi Keselamatan Dalam Pembangunan Sistem.....	95
10.2.2 Prosedur Kawalan Perubahan Sistem	95
10.2.3 Semakan Teknikal Aplikasi Selepas Perubahan Platform	96
10.2.4 Kawalan Terhadap Perubahan Kepada Perisian	97
10.2.5 Prinsip Kejuruteraan Sistem Yang Selamat.....	97
10.2.6 Persekitaran Pembangunan Sistem Yang Selamat	97
10.2.7 Pembangunan Sistem Secara Luaran	97
10.2.8 Ujian Keselamatan Sistem.....	98



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

10.2.9 Pengekodan Selamat (<i>Secure Coding</i>)	99
10.3 Data Ujian.....	99
10.3.1 Perlindungan Data Ujian	99
BAB 11: HUBUNGAN DENGAN PEMBEKAL.....	100
11.1 Keselamatan Maklumat dalam Hubungan Pembekal.....	100
11.1.1 Polisi Keselamatan Maklumat ke atas Pembekal	100
11.1.2 Kawalan Keselamatan Maklumat Melalui Perjanjian dengan Pembekal	101
11.1.3 Kawalan Keselamatan Maklumat Dengan Pembekal dan Pihak Ketiga	101
11.2 Pengurusan Penyampaian Perkhidmatan Pembekal	101
11.2.1 Pemantauan dan Penilaian Perkhidmatan Pembekal.....	101
11.2.2 Pengurusan Perubahan Perkhidmatan Pembekal	101
11.3 Keselamatan Maklumat Dalam Pengurusan Projek	102
11.3.1 Pengurusan Projek.....	102
11.3.2 Keselamatan Maklumat Dalam Pengurusan Projek	103
BAB 12: PENGURUSAN INSIDEN KESELAMATAN ICT	106
12.1 Pengurusan Insiden Dan Penambahbaikan Keselamatan Maklumat.....	106
12.1.1 Tanggungjawab Dan Prosedur	106
12.1.2 Pelaporan Insiden Keselamatan Maklumat.....	106
12.1.3 Pelaporan Kelemahan Keselamatan Maklumat	107
12.1.4 Penilaian dan Keputusan Insiden Keselamatan Maklumat	109
12.2 Pelantikan Pegawai Bertanggungjawab	110
12.3 Pengumpulan dan Pengendalian Bukti.....	111
BAB 13: PENGURUSAN KESINAMBUNGAN PERKHIDMATAN (PKP)	
(BUSINESS CONTINUITY MANAGEMENT (BCM)).....	113
13.1 Kesenambungan Perkhidmatan	113
13.2 Pelan Kesenambungan Perkhidmatan (<i>Business Continuity Plan (BCP)</i>).....	113
13.3 Perubahan atau Pengecualian PKP	114
13.4 Program Latihan dan Kesedaran Terhadap PKP	114
13.5 Pengujian PKP	114



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

13.6 Ketersediaan Kemudahan Pemprosesan Maklumat	115
BAB 14: PEMATUHAN	116
14.1 Pematuhan Polisi	116
14.2 Keperluan Perundangan	116
14.3 Perlindungan dan Privasi Data Peribadi	116
14.4 Semakan Keselamatan Maklumat	117
14.5 Pelanggaran Perundangan	118
14.6 Akuan Pematuhan Polisi Keselamatan Siber	118
14.7 Pematuhan Terhadap Hak Harta Intelek (Intellectual Property Rights)	118
Bab 15: Risikan Ancaman (Threat Intelligence)	119
15.1 Keperluan Risikan Ancaman	119
KAKITANGAN JABATAN	121
LAMPIRAN A (I)	121
PEMBEKAL/ PIHAK KETIGA	123
LAMPIRAN A (II), B (I) & B (II)	123
RUJUKAN	127



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

SEJARAH DOKUMEN POLISI KESELAMATAN SIBER

VERSI	KELULUSAN	TARIKH KUAT KUASA
1.0	JPICT JKPTG	12 September 2024
2.0	JPICT JKPTG	15 Oktober 2025



Pengenalan

Polisi Keselamatan Siber (PKS) Jabatan mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi semasa menggunakan aset Teknologi Maklumat dan Komunikasi atau Information Technology and Communication (ICT). Polisi ini juga menerangkan kepada pengguna mengenai tanggungjawab dan peranan pengguna dalam melindungi aset ICT Jabatan.

Objektif

PKS jabatan diwujudkan untuk menjamin kesinambungan urusan jabatan dengan meminimumkan kesan insiden keselamatan ICT. Polisi ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi jabatan. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi dengan baik. Objektif utama PKS ini diwujudkan adalah seperti berikut:

- a) Memastikan kelancaran operasi jabatan dan meminimumkan kerosakan atau kemusnahan;
- b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan
- c) Mencegah salah guna atau kecurian aset ICT Kerajaan.



PENYATAAN POLISI

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah. Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT.

Terdapat empat (4) komponen asas keselamatan ICT iaitu:

- a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;
- b) Menjamin setiap maklumat adalah tepat dan sempurna;
- c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
- d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

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

- a) **KERAHSIAAN** - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
- b) **INTEGRITI** - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;
- c) **TIDAK BOLEH DISANGKAL** - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- d) **KESAHIHAN** - Data dan maklumat hendaklah dijamin kesahihannya; dan
- e) **KETERSEDIAAN** - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP

Skop PKS jabatan meliputi perkara berikut:

- a) **Maklumat:** Pangkalan data dan fail data, kontrak dan perjanjian, sistem dokumentasi, maklumat penyelidikan, manual pengguna, bahan latihan, prosedur operasi dan sokongan, pelan kesinambungan perkhidmatan, fallback arrangements, jejak audit (audit trails) dan maklumat arkib;
- b) **Platform Aplikasi dan Perisian:** Perisian aplikasi, perisian sistem, alat pembangunan (development tools) dan utiliti (utilities);
- c) **Peranti Fizikal dan Sistem:** Peralatan komputer, peralatan komunikasi, media mudah alih dan lain-lain peralatan;
- d) **Aliran Data:** Merujuk kepada aliran transaksi data menggunakan saluran komunikasi yang dikenal pasti, direkodkan dan dikaji semula secara berkala seperti e-mel rasmi;
- e) **Sistem Luaran:** Sistem bukan milik Jabatan yang dihubungkan dengan sistem Jabatan;
- f) **Sumber Luaran:** Perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi Jabatan seperti perkhidmatan pengkomputeran dan komunikasi, utiliti umum seperti pencahayaan, elektrik dan pendingin hawa;
- g) **Manusia:** Kelayakan, kemahiran dan pengalaman; dan



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

h) **Aset tidak nyata (intangibles):** Seperti reputasi dan imej organisasi.

Semua warga jabatan adalah bertanggungjawab memastikan dan memulihara maklumat dan data berdasarkan perkara berikut:

- a) Maklumat dan data hendaklah boleh dicapai secara berterusan dengan cepat, tepat, mudah dan dengan cara yang diyakini selamat bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.
- b) Semua maklumat dan data hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta melindungi kepentingan jabatan, perkhidmatan dan masyarakat.
- c) Mengenalpasti semua maklumat dan data yang dijana atau dikumpul oleh dan diasingkan mengikut kategori maklumat seperti Maklumat Rahsia Rasmi, Maklumat Rasmi, Maklumat Pengenalan Diri dan Data Terbuka.
- d) Bagi memastikan keselamatan maklumat yang berterusan, PKS merangkumi perlindungan semua bentuk maklumat dan data kerajaan yang dimasukkan, diwujudkan, dimusnahkan, disimpan, dijana, dicetak, diakses, diedarkan, dalam penghantaran dan yang dibuat salinan keselamatan. Ini dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan/ prosedur dalam pengendalian maklumat dan aset.



PRINSIP-PRINSIP

Prinsip PKS ini adalah seperti berikut:

a) Prinsip Perlu Tahu

Capaian dibenarkan dan dihadkan kepada pengguna tertentu atas dasar “perlu tahu” berdasarkan klasifikasi maklumat dan tahap tapisan keselamatan pengguna.

b) Hak Keistimewaan Minimum

Hak capaian kepada pengguna dimulai pada tahap yang paling minimum. Kelulusan adalah perlu bagi membolehkan capaian pada tahap yang lebih tinggi.

c) Kawalan Capaian Berdasarkan Peranan

Capaian sistem dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentubadalah berdasarkan peranan tersebut.

d) Peminimuman Data

Menghadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.



e) Akauntabiliti

Setiap pengguna adalah bertanggungjawab ke atas semua tindakan terhadap kemudahan ICT jabatan yang disediakan. Tanggungjawab pengguna termasuk perkara berikut:

- i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
- ii. Memeriksa maklumat dan menentukan ianya sentiasa tepat dan lengkap;
- iii. Menentukan maklumat sedia untuk digunakan;
- iv. Menjaga kerahsiaan maklumat; dan
- v. Mematuhi langkah dan garis panduan keselamatan yang ditetapkan.

f) Pengasingan Tugas

Setiap tugas, proses dan persekitaran pelaksanaan ICT hendaklah dipisahkan dan diasingkan sebaik mungkin untuk mengekalkan integriti dan perlindungan keselamatan daripada kesilapan dan penyalahgunaan. Pada tahap minimum, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut:

- i. Persekitaran pembangunan di mana sesuatu aplikasi dalam proses pembangunan;
- ii. Persekitaran penerimaan iaitu peringkat di mana sesuatu aplikasi diuji; dan
- iii. Persekitaran sebenar di mana aplikasi sedia untuk beroperasi.

g) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden atau keadaan yang mengancam keselamatan. Pengauditan adalah penting dalam menjamin akauntabiliti seperti berikut:

- i. Mengesan pematuhan atau pelanggaran polisi keselamatan;



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- ii. Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya pelanggaran polisi keselamatan; dan
- iii. Menyediakan bahan bukti bagi menentukan sama ada berlakunya pelanggaran polisi keselamatan.

h) Pematuhan

Prinsip ini penting untuk mengelak pelanggaran polisi melalui tindakan berikut:

- i. Mewujudkan proses yang sistematik khususnya dalam menjamin keselamatan ICT untuk memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan;
- ii. Merumuskan pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenal pasti;
- iii. Melaksanakan program pemantauan keselamatan secara berterusan untuk memastikan standard, prosedur dan garis panduan keselamatan dipatuhi; dan
- iv. Menguatkuasakan amalan melaporkan sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan.

i) Pemulihan

Pemulihan adalah untuk memastikan ketersediaan dan kebolehcapaian dengan meminimumkan gangguan atau kerugian akibat daripadanya adalah seperti berikut:

- i. Merancang dan menguji Pelan Pemulihan Bencana (DRP); dan
- ii. Melaksanakan amalan terbaik dalam pelaksanaan ICT.



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

j) Saling Bergantung

Prinsip keselamatan adalah saling lengkap melengkapi dan hendaklah dipatuhi bagi jaminan keselamatan yang berkesan. Tindakan mempelbagaikan pendekatan dalam menyusun strategi mekanisme keselamatan mampu meningkatkan tahap keselamatan.



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

SINGKATAN DAN TAKRIFAN

BCM	<i>Business Continuity Management</i>
BCP	<i>Business Continuity Plan</i>
BPK	Bahagian Pentadbiran dan Kewangan
BPM	Bahagian Pengurusan Maklumat
BPSM	Bahagian Pengurusan Sumber Manusia
CCP	<i>Communication Crisis Plan</i> / Pelan Krisis Komunikasi
CERT	Computer Emergency Response Team
CDO	<i>Chief Digital Officer</i>
CGSO	<i>Chief Government Security Office</i> / Pejabat Ketua Pegawai Keselamatan Kerajaan
CNII	<i>Critical National Information Infrastructure</i> / Prasarana Maklumat Kritikal Negara
CSIRT	<i>Cyber Security Incident Response Team</i>
DDOS	<i>Distributed Denial of Service</i>
DRP	<i>Disaster Recovery Plan</i> / Pelan Pemulihan Bencana
DRC	<i>Disaster Recovery Centre</i> / Pusat Pemulihan Bencana
ERP	<i>Emergency Response Planning</i> / Pengurusan Tindakbalas Kecemasan
GCIRT	<i>Government Computer Emergency Response Team</i>
ICT	<i>Information and Communication Technology</i>
ICTSO	<i>Information and Communication Technology Security Officer</i>
ID	<i>Identity</i>
IDS	<i>Intrusion Detection System</i>
IPS	<i>Intrusion Prevention System</i>
ISMP	<i>Information Security Management Plan</i> / Pelan Pengurusan Keselamatan Maklumat



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

ISMS	<i>Information Security Management System / Sistem Pengurusan Keselamatan Maklumat</i>
JPICT	Jawatankuasa Pemandu ICT
JKOICT	Jawatankuasa Keselamatan dan Operasi ICT
KSU	Ketua Setiausaha
KJ	Ketua Jabatan
LAN	<i>Local Area Network</i>
JDN	Jabatan Digital Negara
NRES	Kementerian Sumber Asli dan Kelestarian Alam
PKI	<i>Public-Key Infrastructure</i>
SMS	<i>Short Message Service</i>
UPS	<i>Uninterruptible Power Supply</i>
VPN	<i>Virtual Private Network</i>
WAN	<i>Wide Area Network</i>



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

BAB 1: PELAKSANAAN POLISI

Objektif: Memastikan hala tuju pengurusan perlindungan maklumat adalah selaras dengan keperluan perkhidmatan jabatan dan peraturan serta undang-undang.

Bil	Perkara
1.1 Pelaksanaan Polisi Keselamatan Siber JKPTG	
	PKS ini dilaksanakan oleh Ketua Jabatan dengan dibantu oleh Jawatankuasa Pemandu ICT yang terdiri daripada CDO, ICTSO dan lain-lain pegawai yang dilantik.
1.2 Pemakaian Polisi	
	PKS ini terpakai kepada semua kakitangan jabatan dan juga pihak ketiga yang berurusan dengan jabatan.
1.3 Penyelenggaraan Polisi	
	PKS ini tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Setiap perubahan hendaklah mendapat pengesahan ICTSO. Perubahan yang melibatkan penambahan atau pemansuhan yang memberi impak ke atas keselamatan adalah dianggap perubahan utama dan hendaklah mendapat pengesahan JPICT Jabatan. Prosedur semakan semula polisi ini adalah seperti berikut: a) Menyemak sekurang-kurangnya dua (2) tahun sekali bagi mengenal pasti dan menentukan perubahan yang diperlukan; b) Mengemukakan cadangan pindaan atau perubahan secara bertulis; dan c) Memaklumkan pindaan atau perubahan polisi yang telah dipersetujui kepada semua pengguna.
Versi: 2.0	
Muka Surat: 20	



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

BAB 2: ORGANISASI KESELAMATAN

Objektif: Menerangkan peranan dan tanggungjawab struktur tadbir urus individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber.

Bil	Perkara
2.1 Organisasi Keselamatan Maklumat	
2.1.1 Peranan dan tanggungjawab Ketua Jabatan	
	Peranan dan tanggungjawab Ketua Jabatan adalah seperti berikut: a) Menetapkan arah tuju dan strategi untuk pelaksanaan keselamatan siber jabatan dan semua cawangan di bawahnya; b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju dan strategi keselamatan siber jabatan dan semua cawangan di bawahnya; c) Merancang, menyelaraskan dan menyeragamkan pelaksanaan program/projek-projek keselamatan siber jabatan dan cawangan di bawahnya supaya selaras dengan Pelan Strategik Pendigitalan jabatan dan kementerian; d) Memastikan keperluan sumber bagi keselamatan siber jabatan adalah mencukupi; dan e) Memastikan pelaksanaan penilaian risiko keselamatan siber jabatan.

Bil	Perkara
Versi: 2.0	Muka Surat: 21



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

2.1.2 Peranan dan tanggungjawab Ketua Pegawai Digital (CDO)

Ketua Jabatan bertanggungjawab melantik CDO di setiap jabatan/ agensi. Peranan dan tanggungjawab CDO adalah seperti berikut:

- a) Membantu Ketua Jabatan dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber;
- b) Menentukan keperluan dan bertanggungjawab ke atas perkara-perkara berkaitan dengan keselamatan siber jabatan; dan
- c) Membangun dan menyelaraskan pelaksanaan program kesedaran dan latihan keselamatan siber.

2.1.3 Peranan dan tanggungjawab Pegawai Keselamatan ICT (ICTSO)

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:

- a) Merancang, melaksana, mengurus dan memantau program keselamatan siber jabatan;
- b) Menguatkuasakan penggunaan PKS;
- c) Memberikan penerangan dan pendedahan berkenaan PKS jabatan kepada pengguna;
- d) Mewujudkan garis panduan dan prosedur selaras dengan keperluan PKS;
- e) Melaksanakan pengurusan risiko keselamatan siber;
- f) Melaksanakan pengauditan, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya;
- g) Memberikan amaran kepada agensi terhadap kemungkinan berlakunya ancaman keselamatan siber seperti virus komputer dan penggodam serta memberi khidmat nasihat dan bantuan teknikal bagi menyediakan langkah perlindungan yang bersesuaian;
- h) Melaporkan insiden keselamatan siber kepada pengurusan jabatan dan kementerian;



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- i) Bekerjasama dengan semua pihak yang berkaitan dalam menangani ancaman atau insiden keselamatan siber dan memperakukan langkah penyelesaian atau pencegahan; dan
- j) Memberi perakuan tindakan tata tertib ke atas pengguna yang melanggar PKS.

2.1.4 Peranan dan tanggungjawab Pengurus ICT

Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:

- a) Memastikan kajian semula dan pelaksanaan kawalan keselamatan siber selaras dengan keperluan jabatan;
- b) Melaporkan ancaman atau insiden keselamatan siber kepada ICTSO;
- c) Menentukan kawalan capaian pengguna terhadap aset ICT; dan
- d) Memastikan penyimpanan rekod, bahan bukti dan laporan ancaman atau insiden keselamatan siber jabatan dilaksanakan dengan berkesan.

2.1.5 Peranan dan tanggungjawab Pentadbir Sistem ICT

Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut:

- a) Menjaga kerahsiaan maklumat keselamatan siber;
- b) Mengambil tindakan segera apabila dimaklumkan mengenai sebarang perubahan pengguna dalaman/ luaran/ asing berkaitan pengurusan ICT;
- c) Menentukan pelaksanaan tahap capaian kemudahan ICT adalah bertepatan dengan arahan pemilik maklumat;
- d) Memantau dan menyediakan laporan aktiviti penggunaan dan capaian pengguna;
- e) Mengenal pasti dan melaporkan aktiviti tidak normal berkaitan ICT kepada pengurus ICT; dan
- f) Menyimpan dan menganalisis rekod jejak audit.



2.1.6 Peranan dan tanggungjawab Pentadbir Rangkaian dan Keselamatan

Pentadbir Rangkaian dan Keselamatan JKPTG ditugaskan kepada Unit Pengurusan Teknikal

Peranan dan tanggungjawab Pentadbir Rangkaian Dan Keselamatan adalah seperti berikut:

- a) memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) beroperasi sepanjang masa;
- b) memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna;
- c) merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada;
- d) mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil;
- e) 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 Kementerian secara tidak sah seperti melalui peralatan modem dan *dial-up*;
- g) Menganalisis log trafik rangkaian dan menyekat aktiviti yang tidak normal.
- h) menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian;
- i) memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian;
- j) Membantu penyediaan Pelan Pemulihan Bencana (DRP); dan
- k) Membantu pelaksanaan simulasi Pelan Pemulihan Bencana (DRP).



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

2.1.7 Peranan dan tanggungjawab Pentadbir Laman Web

Pentadbir Laman Web JKPTG ditugaskan kepada Unit Pengurusan Strategik ICT

Peranan dan tanggungjawab Pentadbir Laman Web Jabatan adalah seperti berikut:

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

2.1.8 Peranan dan tanggungjawab Pentadbir Pangkalan Data

Pentadbir Laman Web JKPTG ditugaskan kepada Unit Pentadbiran Tanah Negeri

Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut:



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- a) melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data;
- b) memastikan pangkalan data beroperasi sepanjang masa dan berada dalam keadaan selamat;
- c) melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data;
- d) memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur;
- e) melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip PKS;
- f) membantu penyediaan Pelan Pemulihan Bencana (DRP);
- g) membantu pelaksanaan simulasi Pelan Pemulihan Bencana (DRP);
- h) melaksanakan proses perkemasan data (*housekeeping*) di dalam pangkalan data;
- i) menganalisis log capaian pangkalan data dan menyekat aktiviti yang tidak normal; dan
- j) melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.

2.1.9 Peranan dan tanggungjawab Pentadbir Pusat Data

Pentadbir Pusat Data ditugaskan kepada Unit Pengurusan Teknikal

Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti berikut:

- a) memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat;
- b) memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data;
- c) menjadualkan dan melaksanakan proses sandaran dan pemulihan ke atas pangkalan data dan sistem secara berkala;



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- d) membantu penyediaan Pelan Pemulihan Bencana (DRP);
- e) membantu pelaksanaan simulasi Pelan Pemulihan Bencana (DRP);
- f) memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan;
- g) melaporkan sebarang pelanggaran keselamatan Pusat Data Kementerian kepada ICTSO; dan
- h) menyediakan laporan semakan pusat data secara berkala; dan
- i) melaksanakan proses replikasi sistem aplikasi kritikal ke Pusat Pemulihan Bencana (DRC).

2.1.10 Peranan dan tanggungjawab Pentadbir Sistem Aplikasi

Pentadbir Sistem Aplikasi ditugaskan kepada Unit Pentadbiran Tanah Negeri

Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut:

- a) memastikan persekitaran sistem aplikasi berada dalam keadaan selamat;
- b) membuat pemantauan dan penyelenggaraan terhadap sistem atau modul dari semasa ke semasa;
- c) memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas;
- d) membantu penyediaan Pelan Pemulihan Bencana (DRP);
- e) membantu pelaksanaan simulasi Pelan Pemulihan Bencana (DRP);
- f) memastikan kod-kod program sistem aplikasi adalah selamat daripada penggadam sebelum sistem tersebut diaktifkan penggunaannya;
- g) menyimpan dan menganalisis rekod jejak audit;
- h) memastikan *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi dikemas kini supaya terhindar daripada ancaman virus dan penggadam;



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- i) mengenal pasti aktiviti yang tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran;
- j) membatalkan atau memberhentikan aktiviti yang tidak normal dengan serta merta; dan
- k) melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya.

2.1.11 Peranan dan tanggungjawab Pentadbir E-mel

Pentadbir E-mel ditugaskan kepada Unit Pengurusan Teknikal

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 jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib;
- c) mengesah dan memaklumkan kepada ICTSO sekiranya mengalami insiden keselamatan melalui saluran rasmi.

2.1.12 Peranan dan tanggungjawab Pegawai Aset ICT

Pegawai Aset ICT ditugaskan kepada Unit Pengurusan Teknikal

Pegawai Aset ICT ialah pegawai yang dilantik oleh Pegawai Pengawal.

Peranan dan tanggungjawab Pegawai Aset ICT adalah seperti berikut:

- 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 pengurusan aset Kerajaan yang berkuat



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- kuasa 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 pelaksanaan pemeriksaan, pelupusan dan hapus kira Aset ICT dilaksanakan mengikut keperluan;
 - g) memastikan semua aset ICT Kerajaan diberi tanda pengenalan dengan cara melabel tanda Hak Kerajaan Malaysia dan nama Kementerian/ Bahagian berkenaan di tempat yang mudah dilihat dan sesuai pada aset berkenaan;
 - h) memastikan setiap kerosakan Aset ICT Kerajaan dilaporkan;
 - i) memastikan semua aset ICT Kerajaan ditandakan dengan Nombor Siri Pendaftaran mengikut susunan yang ditetapkan;
 - j) memastikan senarai daftar induk aset ICT Kerajaan disediakan;
 - k) memastikan senarai aset ICT disediakan dan dipaparkan di lokasi;
 - l) memastikan setiap kerosakan aset ICT Kerajaan dilaporkan untuk tujuan penyelenggaraan; dan
 - m) bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan Merekodkan kan penyelenggaraan aset ICT Kerajaan;
 - n) memastikan setiap kes kehilangan Aset ICT Kerajaan dilaporkan dan diuruskan dengan teratur.



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

2.1.13 Peranan dan tanggungjawab Pengguna

Pengguna mempunyai peranan dan tanggungjawab seperti berikut:

- a) Membaca, memahami dan mematuhi PKS jabatan;
- b) Menjaga kerahsiaan maklumat berkaitan penggunaan ICT;
- c) Mengikuti dan menghayati program kesedaran keselamatan siber;
- d) Menandatangani akuan pematuhan PKS seperti di **LAMPIRAN A** atau yang setara dengannya;
- e) Menandatangani Akuan Akta Rahsia Rasmi 1972 seperti di **LAMPIRAN B** atau yang setara dengannya; dan
- f) Melaporkan aktiviti yang tidak normal berkaitan ICT kepada BPM.

2.2 Jawatankuasa Pemandu ICT (JPICT)

Peranan dan tanggungjawab Jawatankuasa Pemandu ICT (JPICT) adalah sebagai struktur organisasi formal yang diwujudkan untuk mengurus dan mematuhi keselamatan siber jabatan seperti berikut:

- a) Komitmen pengurusan atasan ke atas keselamatan siber dilaksanakan dengan aktif dan telus;
- b) Tanggungjawab yang jelas dan jalinan perhubungan/ komunikasi dengan semua pengguna dalam pengurusan keselamatan siber;
- c) Keperluan untuk pengurusan kerahsiaan maklumat dikenal pasti, dilaksana dan dikaji secara berkala; dan
- d) Memastikan kajian semula ke atas keselamatan maklumat dijalankan mengikut peraturan yang ditetapkan.

2.3 Jawatankuasa Keselamatan dan Operasi ICT (JKOICT)

Peranan dan tanggungjawab Jawatankuasa Keselamatan dan Operasi ICT (JKOICT) Jabatan adalah seperti berikut:



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- a) Merancang, melaksana, menyemak dan memantau dasar, strategi dan pelan tindakan operasi dan keselamatan siber jabatan;
- b) Merancang, melaksana, menyelaraskan dan memantau pengurusan operasi dan keselamatan siber jabatan;
- c) Merancang, melaksana, menyelaraskan dan memantau pelaksanaan pelan tindakan komunikasi dan operasi ICT bagi jabatan; dan
- d) Melaporkan kemajuan, penyelarasan dan pemantauan keselamatan siber dan pelaksanaan pelan tindakan komunikasi dan operasi ICT kepada JPICT Jabatan.

2.4 Juruaudit

- a) Mengkaji dan menilai kawalan ke atas pematuhan dan pemantauan keselamatan siber berdasarkan dasar, standard dan prosedur keselamatan maklumat; dan
- b) Menilai kawalan pengurusan keselamatan aset ICT.

2.5 Penasihat Undang-undang

- a) Menyediakan khidmat nasihat perundangan bagi memastikan aktiviti ICT jabatan dapat dijalankan dengan lancar dan berkesan selaras dengan perundangan yang berkuat kuasa;
- b) Menyemak kontrak bagi memastikan terma dan syarat kontrak memelihara kepentingan Kerajaan dan selaras dengan peruntukan perundangan yang sedang berkuat kuasa;
- c) Memberi khidmat nasihat perundangan dalam hal yang berkaitan dengan obligasi serta tanggungan pihak Kerajaan dalam mana-mana kontrak (sekiranya ada); dan
- d) Menyediakan khidmat nasihat perundangan bagi melindungi aset ICT, sumber dan kakitangan jabatan terhadap pelbagai risiko perundangan.



2.6 Pengurus Sumber Manusia

- a) Memaklumkan dasar, polisi, pekeliling dan garis panduan pengurusan sumber manusia berkaitan dengan ICT;
- b) Menyediakan khidmat sokongan pentadbiran bagi urusan menyimpan dan menyelenggarakan maklumat pengurusan sumber manusia berkaitan dengan ICT dengan mematuhi peraturan, undang-undang dan polisi yang berkuat kuasa;
- c) Memaklumkan sebarang pertukaran, perpindahan, persaraan dan atau penamatan perkhidmatan kakitangan kepada pentadbir sistem ICT;
- d) Menyelaras urusan tatatertib dan perkhidmatan sumber manusia; dan
- e) Menghebahkan dasar, polisi, pekeliling dan garis panduan yang berkaitan dengan perjawatan, penilaian prestasi, kemajuan kerjaya, skim gaji dan perkara-perkara lain yang berkaitan dengan perjawatan.

2.7 Pihak Ketiga

- a) Menjaga kerahsiaan maklumat berkaitan penggunaan ICT;
- b) Menandatangani perakuan pematuhan keselamatan siber yang ditetapkan oleh Kerajaan Malaysia atau peraturan yang setara/ berkaitan yang berkuat kuasa;
- c) Melaporkan aktiviti yang tidak normal berkaitan ICT kepada BPM; dan;
- d) Mendapatkan kelulusan untuk menggunakan kemudahan ICT.

2.8 Peranti mudah alih dan *teleworking*

a) Peranti mudah alih milik persendirian

Peranti mudah alih milik persendirian hendaklah dikawal daripada



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

mencapai maklumat Rahsia Rasmi dan hendaklah mematuhi polisi serta prosedur yang ditetapkan untuk dibawa masuk ke kawasan terperingkat.

b) Teleworking

- ii. Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi;
- iii. Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat; dan
- iv. Memastikan bahawa antivirus digunakan dan sentiasa dikemaskinikan untuk aset ICT.



BAB 3: KESELAMATAN SUMBER MANUSIA

Objektif: Memastikan semua pihak yang terlibat dalam pengurusan dan penggunaan ICT hendaklah:

- i. Memahami tanggungjawab dan peranan;
- ii. Meningkatkan pengetahuan dan kesedaran; dan
- iii. Menguruskan aspek keselamatan secara teratur.

Dalam meningkatkan keselamatan penyampaian maklumat dan mengurangkan risiko penyalahgunaan aset ICT semua pihak terlibat hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

Bil	Perkara	Tanggungjawab
3.1 Sebelum Dalam Perkhidmatan		
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Menjelaskan peranan dan tanggungjawab pihak yang terlibat dalam meningkatkan keselamatan penyampaian maklumat dan mengurangkan risiko penyalahgunaan aset ICT sebelum, semasa dan selepas perkhidmatan; b) Menjalankan tapisan keselamatan untuk pihak yang terlibat selaras dengan keperluan perkhidmatan, mengikut peraturan sedia ada; dan	ICTSO/ Pengurus ICT/ Pengurus Sumber Manusia/ Pengguna/ Pihak Ketiga



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan dan ditandatangani.

3.2 Semasa Dalam Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- a) Memastikan pihak terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani perjanjian ketakdedahan seperti Arahan Keselamatan. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan;
- b) Memastikan pihak yang terlibat mematuhi keselamatan siber berdasarkan kepada dasar dan peraturan yang ditetapkan oleh Kerajaan;
- c) Memastikan tindakan disiplin atau undang-undang dilaksanakan sekiranya berlaku pelanggaran peraturan yang ditetapkan;
- d) Memastikan tanggungjawab dan peranan dalam pengurusan keselamatan siber dinyatakan dalam senarai tugas yang merangkumi:
 - i. Tanggungjawab kakitangan;

ICTSO/
Pengurus ICT/
Pengurus
Sumber
Manusia/
Pengguna/
Pihak Ketiga



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- ii. Hubungan dengan pegawai atasan; dan
 - iii. Tanggungjawab kakitangan dalam keselamatan siber.
-
- e) Kakitangan haruslah diberi latihan yang bersesuaian dan berterusan dalam semua aspek keselamatan siber yang berkaitan dengan tugas mereka;
 - f) Kakitangan bertanggungjawab mengikuti latihan pengurusan keselamatan siber berdasarkan keperluan;
 - g) Ketua Jabatan atau Ketua Bahagian bertanggungjawab mengkaji semula keperluan latihan untuk setiap kakitangan di bawahnya;
 - h) Program kesedaran keselamatan siber juga perlu dilaksanakan secara berterusan sebagai langkah peringatan kepada kakitangan jabatan berkenaan kepentingan keselamatan aset ICT jabatan; dan
 - i) Mengikuti program kesedaran keselamatan siber secara berkala sekurang-kurangnya satu (1) kali setahun.

3.3 Bertukar/ Tamat Perkhidmatan/ Cuti Belajar

Perkara-perkara yang perlu dipatuhi adalah seperti berikut berikut:

ICTSO/ Pentadbir
Sistem/Pengguna/Pihak
Ketiga



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- | | | |
|--|---|--|
| | <p>a) Memastikan semua aset ICT dikembalikan kepada jabatan mengikut peraturan dan atau terma perkhidmatan yang ditetapkan; dan</p> <p>b) Membatalkan atau menarik balik semua kebenaran capaian ke atas aset ICT mengikut peraturan yang ditetapkan.</p> | |
|--|---|--|



BAB 4: PENGURUSAN ASET

Objektif: Memastikan setiap aset hendaklah dikenal pasti, dikelas, direkod dan diselenggara untuk memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT.

Bil	Perkara	Tanggungjawab
4.1 Tanggungjawab Terhadap Aset		
4.1.1 Inventori dan Pemilikan Aset ICT		
	Semua aset ICT di jabatan mestilah diuruskan mengikut peraturan dan tatacara yang berkuat kuasa seperti berikut: a) Setiap aset ICT hendaklah didaftarkan dan ditentukan pemiliknya. Ketua Jabatan atau Ketua Bahagian adalah bertanggungjawab mengenal pasti pemilik aset ICT tersebut; b) Pemilik aset hendaklah menentukan tahap sensitiviti (terperingkat) yang bersesuaian bagi setiap maklumat aset di jabatan. Pemilik aset juga hendaklah membuat keputusan dalam menentukan individu yang dibenarkan untuk capaian dan penggunaan maklumat tersebut; c) Pentadbir aset ICT adalah bertanggungjawab untuk menentukan prosedur kawalan khas (contohnya:	KJ/ Pentadbir Aset ICT/ Pemilik Aset/ Pengguna Aset



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	kawalan capaian), kaedah pelaksanaan dan penyelenggaraan serta menyediakan langkah pemulihan yang konsisten dengan arahan pemilik aset; d) Semua pengguna aset ICT mestilah mematuhi keperluan kawalan yang telah ditetapkan oleh pemilik aset atau pentadbir sistem. Pengguna adalah terdiri daripada kakitangan jabatan (lantikan tetap, pinjaman, kontrak dan sambilan), konsultan, kontraktor atau pihak ketiga yang terlibat secara langsung; e) Kehilangan/ kecurian aset ICT mestilah dilaporkan serta merta mengikut prosedur pengurusan kehilangan/ kecurian aset berpandukan Arahan Perbendaharaan yang telah ditetapkan; f) Senarai maklumat aset di jabatan hendaklah diwujudkan. Setiap aset perlu ditentukan dengan jelas dan pemilikan aset mestilah dipersetujui dan didokumenkan berserta lokasi semasa aset tersebut. Senarai aset hendaklah disimpan oleh Ketua Jabatan atau Ketua Bahagian; dan g) Setiap pengguna adalah bertanggungjawab terhadap apa-apa kekurangan, kerosakan atau kehilangan aset KJ/ Pentadbir Aset h) ICT/ Pemilik Aset/	
--	---	--



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- i) Pengguna Aset ICT di bawah tanggungannya.

4.1.2 Peralatan Mudah Alih dan Kerja Jarak Jauh

Perkara yang perlu dipatuhi bagi memastikan keselamatan peralatan mudah alih dan kerja jarak jauh terjamin adalah seperti berikut:

- a) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi;
- b) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat;
- c) Memastikan bahawa antivirus digunakan dan sentiasa dikemaskinikan untuk aset ICT;
- d) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan
- e) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.

KJ/ Pentadbir Aset
ICT/ Pemilik Aset/
Pengguna Aset

4.1.3 Peminjaman dan Pemulangan Aset ICT

Peminjaman

KJ/ Pentadbir Aset
ICT/ Pemilik



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	Langkah-langkah yang perlu diambil termasuklah seperti berikut: a) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh jabatan 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 e) pemulangan dilakukan. <u>Pemulangan</u> Memastikan semua aset ICT dikembalikan kepada jabatan mengikut peraturan dan atau terma perkhidmatan yang ditetapkan bagi pegawai yang: a) Bertukar keluar; b) Bersara; c) Ditamatkan perkhidmatan; dan d) Diarahkan oleh Ketua Jabatan. Membatalkan atau menarik balik semua kebenaran capaian ke atas aset ICT mengikut peraturan yang ditetapkan.	Aset/ Pengguna Aset
--	--	----------------------------



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

4.2 Pengelasan, Pelabelan dan Pengendalian Maklumat

4.2.1 Pengelasan Maklumat

	Pengelasan maklumat bertujuan memastikan setiap maklumat diberi perlindungan oleh pemilik aset untuk menentukan keperluan, keutamaan dan tahap keselamatan berdasarkan peraturan yang berkuat kuasa seperti berikut: a) Rahsia Besar; b) Rahsia; c) Sulit; d) Terhad; dan e) Data Terbuka.	KJ/ Pentadbir Aset ICT/ Pemilik Aset/ Pengguna Aset
--	---	--

4.2.2 Pelabelan dan Pengendalian Maklumat

	Semua maklumat mestilah dilabelkan mengikut klasifikasi maklumat seperti yang dinyatakan pada para 4.2.1 Pengelasan Maklumat. a) Aktiviti yang melibatkan pemprosesan maklumat seperti penyalinan, penyimpanan, penghantaran (sama ada dari segi lisan, pos, faksimile dan mel elektronik) dan pemusnahan maklumat mestilah mengikut standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; dan b) Maklumat yang diklasifikasikan sebagai Rahsia Besar, Rahsia, Sulit dan Terhad perlu dilindungi daripada didedahkan kepada pihak ketiga atau awam. Pihak	Pentadbir Aset/ Pemilik Aset
--	---	---



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

ketiga jika perlu boleh diberi kebenaran capaian maklumat jabatan atas dasar perlu tahu sahaja dan mestilah mendapat kebenaran daripada jabatan.

4.3 Pengendalian Media Penyimpanan Maklumat

Perkara-perkara yang mesti dipatuhi adalah seperti berikut:

- a) Memastikan tidak berlaku pendedahan, pengubahsuaian, peralihan atau pemusnahan aset secara tidak sah dan yang boleh mengganggu aktiviti perkhidmatan;
- b) Prosedur perlu disediakan untuk pengurusan peralatan penyimpanan maklumat mudah alih;
- c) Peralatan penyimpanan maklumat yang tidak digunakan perlu dilupuskan secara selamat mengikut prosedur yang telah ditetapkan;
- d) Prosedur untuk mengendali dan menyimpan maklumat perlu diwujudkan untuk melindungi maklumat daripada didedah tanpa kebenaran atau disalah guna;
- e) Dokumentasi sistem perlu dilindungi daripada capaian yang tidak dibenarkan;
- f) Polisi, prosedur dan kawalan pertukaran maklumat yang rasmi perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis

Ketua Jabatan/
Pentadbir Aset



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	kemudahan komunikasi dalam agensi dan mana-mana pihak terjamin; g) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara agensi dengan pihak luar; h) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari agensi; i) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya; dan j) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem maklumat agensi.	
--	--	--



BAB 5: PENGURUSAN KAWALAN CAPAIAN

Objektif: Mengawal Capaian Maklumat.

Bil	Perkara	Tanggungjawab
5.1 Keperluan Kawalan Capaian		
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; d) Kawalan ke atas kemudahan had capaian maklumat; dan	Pentadbir Rangkaian/ Pentadbir Sistem/ Pengguna



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- e) Kawalan capaian perlu dilaksanakan bersama kawalan fizikal dan persekitaran.

5.2 Kawalan Capaian Rangkaian

Polisi akses kepada rangkaian dan servis rangkaian yang konsisten dengan polisi kawalan capaian perlu diwujudkan dan merangkumi:

- a) Rangkaian dan servis rangkaian yang diberikan kebenaran akses sahaja;
- b) Prosedur penentuan pengguna yang diberi akses;
- c) Pengurusan kawalan dan prosedur untuk melindungi rangkaian;
- d) Keperluan pengesahan pengguna untuk akses kepada servis rangkaian; dan
- e) Pemantauan penggunaan servis rangkaian.

Pentadbir
Rangkaian/
Pentadbir Sistem/
Pengguna

5.3 Pengurusan Capaian Pengguna

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Mewujudkan prosedur pendaftaran dan pembatalan kebenaran kepada pengguna untuk mencapai maklumat dan perkhidmatan;
- b) Akaun pengguna adalah unik dan pengguna bertanggungjawab ke atas

Pentadbir
Rangkaian/
Pentadbir Sistem/
Pengguna



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	akaun tersebut selepas pengesahan penerimaan dibuat; c) Akaun pengguna yang diwujudkan dan tahap capaian termasuk sebarang perubahan mestilah mendapat kebenaran secara bertulis dan direkodkan; d) Pemilikan akaun dan capaian pengguna adalah tertakluk kepada peraturan jabatan dan tindakan pengemaskinian dan atau pembatalan hendaklah diambil atas sebab seperti berikut: i. Pengguna tidak hadir bertugas tanpa kebenaran melebihi dari tujuh (7) hari; ii. Pengguna bercuti atau bertugas di luar pejabat mengikut peraturan yang berkuat kuasa; iii. Pengguna bertukar jawatan, tanggungjawab dan atau bidang tugas. Pembatalan akan dilakukan di hari terakhir pertukaran tersebut; iv. Pengguna yang sedang dalam prosiding dan atau dikenakan tindakan tatatertib oleh pihak berkuasa tatatertib. Pembatalan akan dilakukan serta merta apabila dimaklumkan oleh pihak	
--	--	--



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	yang mengendalikan pengurusan sumber manusia; dan v. Pengguna bertukar, berpindah, bersara dan atau tamat perkhidmatan. Pembatalan akan dilakukan berdasarkan tarikh arahan yang dikeluarkan oleh Bahagian Pengurusan Sumber Manusia (BPSM). e) Aktiviti capaian oleh pengguna direkod dan diselenggarakan dengan sistematik dari semasa ke semasa. Maklumat yang di rekod termasuk identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh, masa, rangkaian dilalui, aplikasi diguna dan aktiviti capaian secara sah atau sebaliknya; dan f) Akaun pengguna yang baru diwujudkan perlu diberikan kata laluan sementara dan pengguna perlu menukar kata laluan apabila log masuk dibuat pada kali pertama.	
--	---	--

5.4 Kawalan Capaian Sistem dan Aplikasi

	Kawalan capaian sistem dan aplikasi perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. a) Kaedah-kaedah yang digunakan	Pentadbir ICT/ Pengguna
--	--	------------------------------------



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

hendaklah mampu menyokong perkara-perkara berikut:

- i. Menyediakan kaedah yang sesuai untuk pengesahan capaian (*authentication*); dan
 - ii. Mengehadkan tempoh penggunaan mengikut kesesuaian.
- b) Perkara-perkara yang perlu dipatuhi adalah seperti berikut:
- i. Menamatkan sesuatu sesi yang tidak aktif sekiranya tidak digunakan bagi satu tempoh yang ditetapkan; dan
 - ii. Mengehadkan tempoh sambungan ke sesuatu aplikasi berisiko tinggi.
- c) Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara berikut hendaklah dipatuhi:
- i. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;
 - ii. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- direkodkan (sistem log);
- iii. Mengehadkan capaian sistem dan aplikasi kepada lima (5) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;
 - iv. Menyediakan mekanisme perlindungan bagi menghalang capaian tidak sah ke atas aplikasi dan maklumat;
 - v. Mewujudkan persekitaran pengkomputeran yang khusus dan terasing untuk sistem maklumat terperingkat (sulit/rahsia); dan
 - vi. Pengguna digalakkan membuat enkripsi dengan menukarkan teks biasa (*plain text*) kepada bentuk *cipher text* ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.

5.5 Pengurusan Kata Laluan

- Sistem pengurusan kata laluan perlu:
- a) Memastikan penggunaan ID pengguna dan kata laluan tidak dikongsi;
 - b) Membenarkan pengguna menukar kata laluan sendiri;
 - c) Menekankan pilihan kata laluan yang



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- berkualiti;
- d) Mewajibkan pengguna menukar kata laluan apabila log masuk kali pertama;
 - e) Menyimpan rekod bagi kata laluan terdahulu dan mengelakkan penggunaan kata laluan yang berulang;
 - f) Tidak memaparkan kata laluan di skrin ketika log masuk;
 - g) Menyimpan kata laluan di dalam fail yang berasingan dengan fail data aplikasi; dan
 - h) Mewajibkan pengguna menukar kata laluan sekurang-kurangnya setiap tiga (3) bulan untuk ke semua sistem utama.

5.6 Pengurusan Kata Laluan Super Administrator

Pentadbir ICT bagi pengurusan kata laluan Super Administrator perlu:

Pentadbir ICT/ Ketua Jabatan

- a) Memastikan penggunaan ID pengguna dan kata laluan tidak dikongsi;
- b) Menekankan pilihan kata laluan yang berkualiti. Merujuk klausa 5.7 (g);
- c) Menyimpan kata laluan di dalam sampul surat yang ditutup di dalam peti besi; dan
- d) Menukar kata laluan sekurang-kurangnya setiap 12 bulan untuk semua sistem utama.

5.7 Tanggungjawab Pengguna

Pengguna perlu mematuhi amalan terbaik penggunaan kata laluan seperti berikut:

Pengguna

- a) Pengguna tidak seharusnya menulis



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

atau menyimpan kata laluan tanpa enkripsi di atas talian melainkan pada kes-kes tertentu di mana ia diperlukan oleh prosedur operasi seperti penyimpanan root ID dan kata laluan bagi sistem utama. Di dalam hal ini, kata laluan haruslah dilindungi dengan menggunakan mekanisme kawalan lain seperti menyimpan kata laluan di dalam laci berkunci dan menggunakan kata laluan yang berbeza bagi capaian berbeza;

- b) Pengguna adalah tidak digalakkan mengguna kata laluan yang sama bagi kegunaan sistem di jabatan mahupun sistem yang tidak terdapat di jabatan;
- c) Pengguna hendaklah tidak mendedahkan kata laluan yang diguna pakai di jabatan kepada sesiapa. Ini termasuklah ahli keluarga dan bukan ahli keluarga apabila melakukan kerja pejabat di rumah. Walau bagaimanapun, bagi ID kata laluan utama yang disimpan di dalam laci berkunci, harus diadakan satu proses mengenai tatacara memperoleh kata laluan berkenaan sekiranya berlaku ketidakhadiran pemegang kata laluan utama sewaktu ia diperlukan;



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- d) Pengguna haruslah menyimpan kata laluan dengan selamat dan tidak dibenarkan berkongsi akaun dengan pengguna lain. Pengguna yang disahkan adalah bertanggungjawab ke atas kerahsiaan dan keselamatan kata laluan dan akaun mereka;
- e) Penggunaan atribut *remember me* adalah tidak dibenarkan sama sekali. Sekiranya akaun atau kata laluan disyaki telah dicerobohi, maka laporan kejadian hendaklah dilaporkan kepada pasukan jabatan *Cyber Security Incident Response Team* (CSIRT) dan tindakan menukar kata laluan perlu dilakukan;
- f) Menggunakan kata laluan yang sukar diramal. Kata laluan adalah bukan perkataan di dalam mana-mana bahasa, dialek, loghat dan sebagainya. Kata laluan tidak seharusnya berdasarkan maklumat peribadi, nama ahli keluarga dan seumpamanya; dan
- g) Sistem pengurusan kata laluan hendaklah menekankan pilihan kata laluan yang berkualiti. Kata laluan yang berkualiti antara lainnya mempunyai ciri ciri seperti berikut:
 - i. Gabungan minimum lapan (8) aksara yang mengandungi kombinasi antara huruf,



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

nombor dan simbol (seperti: 0-9, a-z, A-Z, ! @ # \$ % ^ & * () - +) ; dan

- ii. Kata laluan yang ditentukan oleh pengguna hendaklah tidak digunakan semula. Pengguna haruslah tidak membina kata laluan yang sama atau seakan-akan serupa seperti mana yang pernah digunakan sebelum ini di tempat lain. Khususnya, lima (5) kata laluan yang pernah digunakan sebelum ini tidak digunakan semula.



BAB 6: KRIPTOGRAFI

Objektif: Kerahsiaan, integriti data, jaminan pengesahan sumber data, tanpa-sangkalan dan jaminan pengesahan entiti.

Bil	Perkara	Tanggungjawab
6.1 Kriptografi		
	Kriptografi bermaksud sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja. Tindakan melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi yang boleh dilakukan adalah seperti berikut: a) Penggunaan enkripsi dengan menukarkan teks biasa (<i>plain text</i>) kepada bentuk <i>cipher text</i> ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa; b) Penggunaan fungsi <i>hash</i> dan Kod Pengesahan Mesej (MAC); c) Penggunaan tandatangan digital digalakkan kepada semua pengguna yang menguruskan transaksi maklumat rahsia rasmi secara elektronik; d) Pengurusan ke atas <i>Public Key</i>	Pemilik Aset/ Pengguna Aset
Versi: 2.0		Muka Surat: 55



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	<i>Infrastructure</i> (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut; e) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan f) Kawalan ke atas kemudahan had capaian maklumat.	
6.2 Data Masking		
	Untuk mengehadkan pendedahan data sensitif termasuk maklumat data peribadi (PII), dan mematuhi keperluan undang-undang, peraturan dan kontrak. Sekiranya pemprosesan melibatkan data sensitif termasuk maklumat data peribadi (contohnya PII), pihak JKPTG hendaklah mempertimbangkan untuk menyembunyikan data tersebut. Teknik-teknik yang boleh digunakan untuk Data Masking termasuk, tetapi tidak terhad kepada: a) Pseudonymization b) Anonymization c) Enkripsi (memerlukan pengguna yang diberi kuasa untuk mempunyai kunci); d) Membatalkan (nulling) atau memadamkan aksara (menghalang pengguna yang tidak dibenarkan	Pentadbir Sistem ICT



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- daripada melihat mesej penuh);
- e) Nombor dan tarikh yang berbeza-beza;
 - f) Penggantian (mengubah satu nilai bagi yang lain untuk menyembunyikan data sensitif); atau
 - g) Menggantikan nilai dengan fungsi hash

6.3 Pencegahan Kebocoran Data (DLP)

Untuk mencegah pendedahan dan pengestrakan maklumat yang tidak dibenarkan oleh individu atau sistem.

- a) Kawalan perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran; dan
- b) Langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

Pentadbir Sistem
ICT



BAB 7: KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif: Memastikan premis dan kemudahan ICT ditempatkan di kawasan yang selamat dan dilindungi daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

Bil	Perkara	Tanggungjawab
7.1 Keselamatan Persekitaran		
7.1.1 Keselamatan Fizikal		
	Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh premis. Langkah-langkah keselamatan fizikal adalah seperti berikut: a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b) Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan dan kunci harus disimpan oleh pegawai bertanggungjawab; c) Memperkukuhkan dinding dan	CGSO/ Pegawai Keselamatan/ CDO/ ICTSO



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	siling; d) Memasang alat penggera dan sistem CCTV; e) Menghadkan jalan keluar masuk; f) Mengadakan kaunter kawalan; g) Menyediakan tempat atau bilik khas untuk pelawat pelawat; h) Mewujudkan perkhidmatan kawalan keselamatan; i) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang mendapat kebenaran sahaja untuk masuk; j) Merekabentuk dan melaksanakan perlindungan fizikal daripada bencana seperti kebakaran, banjir, letupan atau huru hara; k) Menyediakan garis panduan keselamatan untuk kakitangan yang bekerja di dalam kawasan terhad; l) Sistem kawalan kunci dengan menetapkan pegawai yang bertanggungjawab untuk menyimpan kunci dengan baik dan mempunyai rekod; dan m) Mewujudkan kawalan di kawasan penghantaran, pemunggahan dan kawasan larangan.	
--	--	--



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

7.1.2 Kawalan Masuk Fizikal

	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap pengguna hendaklah memakai pas keselamatan sepanjang waktu bertugas; b) Setiap pelawat mestilah mendaftar dan mendapatkan pas pelawat di pintu masuk utama jabatan untuk ke kawasan/ tempat berurusan dan hendaklah dikembalikan semula selepas tamat urusan; c) Semua pas keselamatan hendaklah diserahkan semula kepada jabatan apabila pengguna bertukar, berhenti atau bersara; dan d) Kehilangan pas keselamatan mestilah dilaporkan dengan segera kepada pegawai keselamatan jabatan.	Pengguna/ Pelawat
--	--	-------------------

7.1.3 Kawasan Larangan

	Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di jabatan adalah di Bilik Pusat	ICTSO/ Pengguna/ Pihak Ketiga/ Pelawat
--	--	--



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- Data, Bilik Fail dan lain-lain.
- a) Akses kepada kawasan tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja;
 - b) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal dan mendapat kebenaran untuk temujanji. Mereka hendaklah diiringi sepanjang masa sehingga tugas atau temujanji di kawasan berkenaan selesai;
 - c) Semua aktiviti pihak ketiga di kawasan larangan perlu mendapat kebenaran daripada pegawai yang diberi kuasa dan dipantau serta dikawal oleh pegawai bertanggungjawab;
 - d) Peralatan/ media perakaman/ storan/ komunikasi adalah tidak dibenarkan dibawa masuk ke dalam pusat data; dan
 - e) Aktiviti mengambil gambar, merakam video, merekodkan suara atau penggunaan peralatan yang tidak berkenaan adalah dilarang.



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

7.1.4 Pemantauan Keselamatan Fizikal

	Premis fizikal perlu dipantau menggunakan sistem pengawasan (contoh: pengawal, penggera pencerobohan, sistem pemantauan video seperti CCTV, sistem aplikasi pengurusan maklumat keselamatan fizikal atau mana-mana yang bersesuaian. Akses ke lokasi kritikal perlu dipantau secara berterusan bagi mengesan akses yang tidak sah atau tingkah laku yang mencurigakan.	CDO, ICTSO, Pengurus ICT
--	--	--------------------------

7.2 Keselamatan Peralatan ICT dan Maklumat

	Melindungi peralatan ICT dan maklumat dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.
--	--

7.2.1 Peralatan ICT

	Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan dengan mengambil tindakan berikut: a) Pengguna mesti mendapat kebenaran daripada ICTSO atau pegawai yang diberikan kuasa untuk membuat instalasi perisian tambahan; b) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif	Pengguna/ Pentadbir Sistem ICT/ Pihak Ketiga/ ICTSO/ Pegawai Aset
--	--	---



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

(*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;

- c) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;
- d) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptible Power Supply* (UPS);
- e) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;
- f) Peralatan ICT yang hendak dibawa keluar dari premis jabatan untuk tujuan rasmi, perlu mendapat kelulusan pegawai yang diberikan kuasa dan direkodkan bagi tujuan pemantauan;
- g) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;
- h) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;
- i) Pengguna mesti mendapat



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	kebenaran daripada ICTSO atau pegawai yang diberikan kuasa untuk mengubah kedudukan komputer dari tempat asal; j) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada pegawai yang bertanggungjawab untuk dibaik pulih; k) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; l) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; m) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (administrator password) yang telah ditetapkan oleh Pentadbir Sistem ICT; n) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; o) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "OFF" apabila meninggalkan pejabat; p) Memastikan plug dicabut	
--	--	--



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

daripada suis utama (main switch) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.

Semua pihak yang terlibat dalam pengurusan atau penggunaan aset ICT hendaklah bertanggungjawab dan mematuhi perkara berikut:

- a) Memastikan semua aset ICT dikembalikan mengikut peraturan dan terma yang ditetapkan; dan
- b) Membatalkan atau menarik balik semua kebenaran, capaian ke atas aset ICT mengikut peraturan yang ditetapkan.

7.2.2 Media Storan

- c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;
- d) Merekodkan pergerakan media storan untuk tujuan pinjaman;
- e) Mendapat kelulusan pemilik maklumat terlebih dahulu sebelum menghapuskan maklumat atau kandungan media storan dengan teratur dan selamat;
- f) Semua media storan yang

Pengguna/ Pentadbir
Sistem ICT



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; g) Mengadakan salinan atau penduaan (<i>backup</i>) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h) Perkakasan penduaan (<i>backup</i>) hendaklah diletakkan di tempat yang terkawal; dan i) Sebarang pelupusan hendaklah merujuk kepada tatacara pelupusan.	
--	--	--

7.2.3 Media Tandatangan Digital

	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada pegawai yang bertanggungjawab untuk	Pengguna/ Pentadbir Sistem ICT
--	--	---------------------------------------



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

tindakan seterusnya.

7.2.4 Media Perisian dan Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan jabatan; Sistem aplikasi dalaman tidak dibenarkan dibentangkan atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT;
- b) Lesen perisian (*registration code*, *CD-keys* dan nombor siri) perlu disimpan berasingan daripada *CD ROM*, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan
- c) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.

ICTSO/ Pentadbir
Sistem/ Pengguna

7.2.5 Penyelenggaraan Peralatan ICT

Peralatan ICT hendaklah diselenggarakan dengan baik bagi memastikan kerahsiaan, integriti dan kebolehsediaan.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh

Pengguna/ Pentadbir
Sistem/ Pihak Ketiga



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	pengeluar; b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	
7.2.6 Pinjaman Peralatan ICT		
	Peralatan ICT yang dipinjam adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mendapatkan kelulusan mengikut peraturan di bawah Pekeliling Perbendaharaan Tatacara Pengurusan Aset atau peraturan jabatan bagi membawa keluar peralatan atau maklumat tertakluk kepada tujuan yang dibenarkan; b) Pengguna hendaklah memohon	Pengguna/ Pentadbir Sistem/ Pihak Ketiga
Versi: 2.0		Muka Surat: 68



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	peminjaman peralatan ICT melalui sistem yang berkuat kuasa; c) Pengguna perlu melindungi dan mengawal peralatan sepanjang tempoh pinjaman; d) Memastikan aktiviti pinjaman dan pemulangan peralatan ICT direkodkan; dan e) Memastikan peralatan ICT yang dipulangkan dalam keadaan baik dan lengkap.	
--	--	--

7.2.7 Peralatan ICT di Luar Premis Jabatan

	Bagi peralatan ICT yang dibawa keluar dari premis, langkah-langkah keselamatan berikut hendaklah diambil a) Peralatan ICT perlu dilindungi dan dikawal sepanjang masa; b) Penyimpanan atau penempatan peralatan ICT mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan c) Memeriksa dan memastikan peralatan ICT yang dibawa keluar tidak mengandungi maklumat Kerajaan. Maklumat perlu dihapuskan dari peralatan tersebut setelah disalin ke media storan sekunder.	Pengguna/ Pegawai Aset/ Pihak Ketiga
--	---	---



7.2.8 Pelupusan Peralatan Aset ICT

	Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa mengikut Tatacara Pengurusan Aset Alih Kerajaan. Pelupusan peralatan ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan jabatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua kandungan peralatan ICT khususnya maklumat terperingkat hendaklah dihapuskan terlebih dahulu sebelum pelupusan dilaksanakan; dan b) Peralatan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat.	Pegawai Aset/ Pengguna
--	--	---------------------------

7.2.9 Clear Desk dan Clear Screen

	Semua maklumat dalam apa jua bentuk media storan hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. <i>Clear Desk</i> dan <i>Clear Screen</i> bermaksud tidak meninggalkan bahan-bahan yang sensitif dan	Pengguna
--	--	----------



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

terperingkat terdedah sama ada di atas meja atau di paparan skrin apabila pemilik tidak berada di tempatnya. Langkah yang perlu diambil adalah dengan menggunakan kemudahan *password screen saver*, *lock PC* atau log keluar apabila meninggalkan komputer.

7.2.10 Perkhidmatan Awan (*Cloud Services*)

Penggunaan aplikasi dan kemudahan infrastruktur pengkomputeran awan (*cloud computing*) tidak dibenarkan sama sekali kecuali pengkomputeran awan yang diluluskan oleh pihak Jabatan/Kerajaan tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa.

Secara asasnya maksud pengkomputeran awan yang dibangun dan dibenarkan oleh pihak Kerajaan adalah perkhidmatan pengkomputeran awan yang dimiliki, diuruskan atau dikendalikan oleh pihak Kerajaan sendiri berdasarkan kepada prinsip, penilaian dan keperluan keselamatan siber secara komprehensif dan strategik melibatkan teknologi, manusia dan proses. Ia bertujuan agar perkhidmatan pengkomputeran awan tersebut memenuhi objektif keselamatan, hala tuju bisnes serta keperluan peraturan

Pengurus ICT dan
Warga JKPTG



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

dan undang undang yang berkuatkuasa. Maklumat yang terlibat dalam transaksi dalam pengkomputeran awan perlu dilindungi daripada aktiviti penipuan dan pendedahan serta pengubahsuaian yang tidak dibenarkan. Penstoran awan ini tertakluk kepada perkhidmatan awan yang dilanggan dan dibenarkan oleh pihak Kerajaan.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Dokumen terperingkat yang disimpan di *public cloud storage* hendaklah menggunakan kaedah enkripsi terlebih dahulu sebelum dimuat naik;
- b) Setiap dokumen yang disimpan dalam talian perlu ditetapkan kata laluan untuk membuka dokumen; dan
- c) Bahan rasmi perlu mendapat kelulusan Ketua Jabatan sebelum dimuat naik ke penstoran awan.

7.2.11 Penghapusan Maklumat

Maklumat yang disimpan di dalam sistem informasi, peralatan dan mana-mana storan media perlu dihapuskan apabila tidak diperlukan. Tatacara penghapusan perlulah mengikut garis panduan dan

Pengurus ICT dan
Warga JKPTG



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

pekeliling yang sedang berkuat kuasa.

7.3 Keselamatan Persekitaran

7.3.1 Kawalan Persekitaran

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

- a) Merancang dan menyediakan pelan keseluruhan susun atur peralatan komputer, ruang atur pejabat dan sebagainya dengan teliti;
- b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;
- c) Peralatan perlindungan keselamatan hendaklah dipasang di tempat yang bersesuaian, mudah dicapai dan dikendalikan;
- d) Bahan mudah terbakar **DILARANG** disimpan di dalam kawasan

ICTSO/ Bahagian
Pentadbiran



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	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, ketuhar gelombang mikro dan lain-lain berhampiran peralatan PC; g) Semua peralatan perlindungan keselamatan hendaklah diperiksa sekurang-kurangnya dua (2) kali setahun dan diuji sekurang-kurangnya satu (1) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; h) Akses kepada bilik sesalur telefon hendaklah sentiasa dikunci; dan i) Mematuhi peraturan yang telah ditetapkan oleh pihak berkuasa seperti Jabatan Bomba dan Penyelamat, Jabatan Kerja Raya dan sebagainya.	
7.3.2 Bekalan Kuasa		
	Bekalan kuasa merupakan punca kuasa	ICTSO/



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan hendaklah disalurkan mengikut *voltage* yang bersesuaian;
- b) Peralatan sokongan seperti *Uninterruptible Power Supply* (UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan; dan
- c) Semua peralatan sokongan bekalan kuasa hendaklah diperiksa dan diuji secara berjadual.

Penyelenggara
Bangunan

7.3.3 Kabel Peralatan ICT

Kabel peralatan ICT hendaklah dilindungi kerana ia adalah salah satu punca maklumat. Langkah-langkah keselamatan kabel adalah seperti berikut:

- a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;
- b) Melindungi kabel dengan menggunakan conduit untuk mengelakkan kerosakan yang disengajakan atau tidak disengajakan;
- c) Melindungi laluan pemasangan

ICTSO/ Pentadbir
Sistem/ Bahagian
Pentadbiran



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan

- d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.

7.3.4 Prosedur Kecemasan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan yang telah ditetapkan;
- b) Melaporkan insiden kecemasan persekitaran kepada Pegawai Keselamatan; dan
- c) Mengadakan, menguji dan mengemaskini pelan kecemasan dari semasa ke semasa.

ICTSO

7.4 Keselamatan Dokumen

Melindungi maklumat dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaiian.

7.4.1 Dokumen

Bagi memastikan integriti maklumat, langkah-langkah pengurusan

ICTSO



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi:

- a) Memastikan sistem dokumentasi atau penyimpanan dokumen adalah selamat dan kehilangan atau kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan;
- b) Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen;
- c) Pergerakan fail terperingkat dan dokumen rahsia rasmi hendaklah mengikut prosedur keselamatan;
- d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara;
- e) Dokumen terperingkat rasmi perlu dienkrapsikan sebelum dihantar secara elektronik; dan
- f) Memastikan cetakan yang mengandungi maklumat terperingkat diambil segera dari pencetak



BAB 8: KESELAMATAN OPERASI

Objektif: Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan baik dan selamat daripada sebarang ancaman dan gangguan.

Bil	Perkara	Tanggungjawab
8.1 Prosedur dan Tanggungjawab Operasi		
	Memastikan pengurusan operasi pemprosesan maklumat dilaksanakan dengan cekap dan selamat.	
8.1.1 Pengendalian Prosedur Operasi		
	Semua prosedur pengurusan operasi hendaklah dikenal pasti, didokumenkan, disimpan dan dihadkan capaian berdasarkan keperluan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua prosedur operasi hendaklah didokumenkan dengan jelas, teratur, dikemaskinikan dan sedia diguna pakai oleh pengguna; b) Setiap perubahan kepada prosedur operasi mestilah dikawal; c) Tugas dan tanggungjawab fungsi perlu diasingkan bagi mengurangkan risiko kecuaiian dan penyalahgunaan aset ICT; dan d) Kemudahan ICT untuk kerja-kerja pembangunan, pengujian dan operasi perlu diasingkan bagi	ICTSO/ Pentadbir Sistem
Versi: 2.0		Muka Surat: 78



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

mengurangkan risiko capaian atau pengubahsuaian secara tidak sah ke atas sistem yang sedang beroperasi.

8.1.2 Pengurusan Perubahan

Perubahan kepada organisasi, proses bisnis, kemudahan pemprosesan maklumat dan sistem yang memberi kesan kepada keselamatan maklumat hendaklah dikawal.

Pengurusan ke atas perubahan perlu diambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Mewujudkan prosedur pengurusan perubahan;
- b) Merekodkan semua perubahan yang telah dipersetujui dan dilaksanakan; dan
- c) Memantau pelaksanaan perubahan.

ICTSO/ Pengguna/
Pentadbir Sistem

8.1.3 Pengurusan Kapasiti

Kapasiti sistem ICT hendaklah dirancang, diurus dan dikawal dengan terperinci bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan operasi sistem ICT. Keperluan kapasiti perlu mengambil kira ciri-ciri keselamatan bagi meminimumkan

ICTSO/
Pentadbir Sistem



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

risiko gangguan kepada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

8.1.4 Pengurusan Konfigurasi

Memastikan peralatan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul dengan aturan keselamatan yang diperlukan dan konfigurasi tidak diubah oleh perubahan yang tidak sah dan tidak betul.

Perkara yang perlu dipatuhi termasuklah mewujudkan, mendokumenkan, melaksana, ICTSO dan Pentadbir memantau dan mengkaji semula konfigurasi keselamatan bagi peralatan, perisian, Sistem ICT perkhidmatan dan rangkaian.

ICTSO dan Pentadbir
Sistem ICT, Pentadbir
Pusat Data,
Pentadbir Rangkaian
ICT, Pentadbir
Pangkalan Data

8.1.5 Pengasingan Kemudahan Pembangunan, Ujian dan Operasi

Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian ataupun perubahan tidak sah ke atas persekitaran operasi.

Perkara–perkara yang perlu dipatuhi:

- a) Mewujudkan prosedur keperluan sumber bagi penyediaan persekitaran untuk pembangunan, pengujian dan operasi;
- b) Merekodkan semua penggunaan

ICTSO/
Pentadbir Sistem



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- sumber yang dilaksanakan; dan
- c) Memantau pelaksanaan penggunaan sumber bagi tujuan perancangan kapasiti.

8.2 Perlindungan daripada *Malware*

8.2.1 Aset ICT perlu dilindungi supaya tidak terdedah kepada kerosakan yang disebabkan oleh kod berbahaya seperti virus, *worm*, *trojan* dan lain-lain.

8.2.2 Kawalan pencegahan, pengesanan dan pemulihan untuk melindungi sistem ICT daripada gangguan *malicious code*. Perkara-perkara yang mesti dipatuhi adalah:

- a) Memasang sistem keselamatan untuk mengesan perisian berbahaya seperti antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS);
- b) Mengimbas semua perisian dengan antivirus sebelum menggunakannya;
- c) Mengemaskinikan paten antivirus dari semasa ke semasa;
- d) Memasang dan menggunakan hanya perisian yang tulen;
- e) Menyemak kandungan sistem ICT secara berkala bagi mengesan aktiviti yang tidak normal seperti manipulasi data tidak sah yang

ICTSO/ Pentadbir Sistem/ Pengguna



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	menyebabkan penambahan, perubahan, kehilangan atau kerosakan maklumat; f) Memasukkan klausa tanggungan ke dalam kontrak yang ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; g) Mewujud dan melaksanakan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; h) Memberi amaran mengenai ancaman seperti serangan virus terhadap keselamatan aset ICT jabatan; i) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya dari semasa ke semasa; j) Melaksanakan Program Kesedaran Pengguna yang bersesuaian; dan k) Penggunaan <i>mobile code</i> yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	
8.3 Backup		
8.3.1	Memastikan kesinambungan perkhidmatan berjalan lancar.	



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

8.3.2	Salinan pendua maklumat dan perisian sistem hendaklah disediakan dan diuji secara berkala selaras dengan polisi backup bagi tujuan kesinambungan operasi pemprosesan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a) Membuat salinan pendua ke atas semua maklumat dan sistem perisian mengikut jadual yang ditetapkan atau apabila berlaku perubahan versi; b) Menyimpan salinan pendua di lokasi lain yang selamat; dan c) Menguji sistem pendua bagi memastikan ianya dapat beroperasi dengan normal.	Pentadbir Sistem
8.4 Log dan Pemantauan		
8.4.1	Semua peristiwa dan bukti kewujudan insiden hendaklah direkodkan untuk tujuan jejak audit.	
8.4.2	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap sistem mestilah mempunyai jejak audit; b) Mewujudkan prosedur untuk memantau penggunaan kemudahan memproses maklumat dan dipantau secara berkala; c) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan	ICTSO/ Pentadbir Sistem



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; d) Maklumat log perlu dilindungi daripada sebarang ubah suai dan capaian yang tidak dibenarkan; e) Sebarang kesalahan, kesilapan atau penyalahgunaan sistem perlu direkodkan, dianalisis dan diambil tindakan sewajarnya; f) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; g) Waktu yang berkaitan dengan sistem pemprosesan maklumat perlu diselaraskan dengan satu sumber waktu yang piawai; dan h) Sebarang aktiviti tidak sah seperti kecurian maklumat dan pencerobohan hendaklah dilaporkan kepada pasukan <i>Cyber Security Incident Response Team</i> (CSIRT).	
8.4.3	Aktiviti Pemantauan	
	Pemantauan kepada rangkaian, sistem dan aplikasi perlu dilaksanakan secara berterusan mengikut tempoh yang bersesuaian. Perkara-perkara yang	ICTSO/ Pentadbir Sistem



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

memerlukan pemantauan termasuklah tetapi tidak terhad kepada:

- a) Trafik keluar masuk rangkaian, sistem dan aplikasi;
- b) Capaian kepada sistem, server, perkakasan rangkaian, sistem pemantauan, sistem aplikasi yang kritikal dan lain-lain;
- c) Tahap pentadbir sistem dan fail konfigurasi rangkaian;
- d) Log dari peralatan/perisian keselamatan (contoh: Antivirus, IDS, IPS, *firewall* dan lain-lain);
- e) Log kejadian berkaitan aktiviti sistem dan rangkaian;
- f) Penggunaan kod yang disahkan tidak disalah guna; dan
- g) Penggunaan sumber (contoh: CPU, *hard disks*, *memory* dan *bandwidth*).

8.5 Kawalan Pengoperasian Perisian

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan jabatan; dan
- b) Lesen perisian (*registration code*, *CD-keys*, nombor siri dan langganan atas talian) perlu disimpan berasingan daripada *CD-ROM*, *disk* atau media berkaitan bagi

Pentadbir Sistem



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

mengelakkan dari berlakunya
kecurian atau cetak rompak.

8.6 Pengurusan Kerentanan Teknikal

8.6.1	Kawalan terhadap sebarang kelemahan teknikal pada perkakasan, sistem pengoperasian dan sistem aplikasi perlu diuruskan secara berkesan, sistematik dan berkala.	Pentadbir Sistem
--------------	---	------------------

8.6.2	Perkara-perkara yang perlu dipatuhi adalah: a) Mengenal pasti maklumat keterdedahan teknikal sistem yang digunakan; b) Menilai tahap keterdedahan bagi mengenal pasti risiko yang bakal dihadapi; dan c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	ICTSO/ Pentadbir Sistem
--------------	---	----------------------------

8.7 Pemakluman Audit

	a) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan; dan b) Capaian ke atas sistem maklumat semasa pengauditan perlu dikawal selia bagi mengelakkan sebarang penyalahgunaan.	Pentadbir Sistem
--	--	------------------



BAB 9: KESELAMATAN KOMUNIKASI

Objektif: Memastikan fasiliti rangkaian serta pengaliran maklumat dalam rangkaian dilindungi sepenuhnya.

Bil	Perkara	Tanggungjawab
9.1 Pengurusan Keselamatan Rangkaian		
	Keselamatan rangkaian adalah elemen penting dalam memastikan pengaliran maklumat lancar dan sempurna.	
9.1.1 Kawalan Infrastruktur Rangkaian		
	Infrastruktur rangkaian hendaklah dirancang, diurus dan dikawal bagi melindungi keselamatan maklumat. Perkara perkara yang mesti dipatuhi adalah: a) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berkaitan dengan sistem rangkaian; b) Peralatan keselamatan seperti <i>firewall</i> hendaklah dipasang bagi memastikan hak capaian ke atas sistem dapat dilaksanakan seperti ditetapkan; c) Sebarang cubaan mencerooboh dan aktiviti yang boleh mengancam sistem dan maklumat jabatan perlu dipantau dan dikesan melalui	ICTSO/ Pentadbir



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	pemasangan peralatan keselamatan seperti <i>Intrusion Prevention System (IPS)</i>; d) Peralatan rangkaian hendaklah diletakkan di lokasi yang bebas dari risiko seperti banjir, gegaran dan habuk; e) Sebarang keperluan penyambungan rangkaian hendaklah melalui proses dan prosedur yang ditetapkan; f) Penggunaan rangkaian tanpa wayar (<i>wireless</i>) LAN di jabatan hendaklah mematuhi peraturan yang dikeluarkan oleh pihak berkenaan seperti JDN dan Majlis Keselamatan Negara (MKN); dan g) Semua perisian berkaitan rangkaian dan keselamatan seperti <i>sniffer</i> atau <i>network analyzer</i> adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO.	
--	--	--

9.1.2 Keselamatan Perkhidmatan Rangkaian

	Perkhidmatan rangkaian hendaklah dipastikan sentiasa selamat bagi memastikan kerahsiaan, integriti dan ketersediaan maklumat terjamin. Perkara-perkara yang perlu dipatuhi adalah:	
--	--	--



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- a) Mekanisme keselamatan, tahap kesediaan perkhidmatan dan keperluan pengurusan perkhidmatan rangkaian hendaklah dikenal pasti dan dinyatakan dalam perjanjian perkhidmatan rangkaian, sama ada perkhidmatan disediakan secara dalaman ataupun menggunakan sumber luar;
- b) Semua trafik keluar dan masuk hendaklah ditapis oleh peralatan keselamatan di bawah kawalan jabatan; dan
- c) Sebarang aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam (PKPA) yang berkuat kuasa perlu disekat melalui penggunaan *Web Content Filtering*.

9.1.3 Web Filtering

Memasang *Web Content Filtering* pada *Internet Gateway* atau kawalan capaian Internet yang bersesuaian untuk menyekat aktiviti/capaian laman web yang dilarang.

Pentadbir

9.1.4 Pengasingan Rangkaian

Pengasingan perkhidmatan rangkaian bertujuan untuk meminimumkan risiko capaian tidak sah dan pengubahsuaian yang tidak dibenarkan. Perkara-perkara

Pentadbir



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

yang perlu dipatuhi adalah:

- a) Mengenal pasti fungsi dan tanggungjawab pengguna;
- b) Mengkonfigurasi hak capaian pengguna mengikut segmen rangkaian berdasarkan keperluan;
- c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;
- d) Mengemaskinikan hak capaian pengguna dari semasa ke semasa mengikut keperluan; dan
- e) Operasi rangkaian hendaklah diasingkan untuk meminimumkan risiko capaian dan pengubahsuaian yang tidak dibenarkan.

9.2 Pemindahan Maklumat

Memastikan keselamatan maklumat terjamin semasa pertukaran maklumat dengan entiti luar.

9.2.1 Prosedur Pemindahan Maklumat

Prosedur ini bertujuan untuk mengendali, menyimpan, memindah serta melindungi maklumat daripada didedah tanpa kebenaran atau salah guna serta memastikan keselamatan pemindahan maklumat dengan entiti luar terjamin. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Menghadkan dan menentukan

ICTSO/ Pengguna/
Pentadbir Sistem



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- capaian kepada pengguna yang dibenarkan sahaja;
- b) Menghadkan pengedaran data untuk tujuan rasmi dan yang dibenarkan sahaja;
- c) Polisi, prosedur dan kawalan pemindahan maklumat yang formal perlu diwujudkan untuk melindungi pemindahan maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;
- d) Sebarang pemindahan maklumat di antara jabatan dan agensi lain mestilah dikawal; dan
- e) Penggunaan perkhidmatan luar seperti aplikasi media sosial dan perkongsian fail untuk pemindahan maklumat rasmi Kerajaan perlu mendapat kelulusan Ketua Jabatan.

9.2.2 Perjanjian Pemindahan dan Kerahsiaan Maklumat

- a) *Non-Disclosure Agreements* (NDA) perlu diwujudkan bagi memastikan kerahsiaan, integriti dan ketersediaan (CIA) maklumat terpelihara semasa proses pemindahan maklumat dan perisian di antara jabatan dengan agensi luar; dan
- b) Keperluan melindungi kerahsiaan meliputi integriti dan kerahsiaan maklumat hendaklah disemak

Agensi/ Pentadbir/
Pihak Ketiga/
Pengguna



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

secara berkala dan didokumenkan.

9.2.3 Pengurusan Mesej Elektronik

Maklumat yang dihantar, diterima dan disimpan melalui mel elektronik perlu dilindungi bagi menghindari capaian atau sebaran maklumat yang tidak dibenarkan. Pengguna layak menerima kemudahan perkhidmatan e-mel dengan kelulusan dari Ketua Setiausaha/ Ketua Jabatan.

KJ/ Agensi/
Pentadbir Sistem/
Pengguna



BAB 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Objektif: Memastikan sistem yang dibangunkan secara dalaman atau pun luaran mempunyai ciri-ciri keselamatan maklumat yang kukuh dan berdaya tahan daripada aktiviti berniat jahat serta merangkumi keseluruhan kitaran hayat aset.

Bil	Perkara	Tanggungjawab
10.1 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat		
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan; b) Semua sistem yang dibangunkan sama ada secara dalaman atau luaran hendaklah dikaji supaya mengikut keperluan pengguna dan selaras dengan dasar atau peraturan berkaitan yang berkuat kuasa; dan c) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan.	JK Penilaian Teknikal/ JPICT/ Pentadbir Sistem/ Pembekal



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

10.1.1 Perlindungan Perkhidmatan Aplikasi yang menggunakan Rangkaian Awam

	Maklumat aplikasi yang menggunakan rangkaian awam hendaklah dilindungi daripada aktiviti tidak sah seperti penipuan, pendedahan maklumat, pengubahsuaian maklumat yang tidak dibenarkan yang menyebabkan pertikaian kontrak. Perkara-perkara yang perlu dipatuhi adalah: a) Identiti pengguna perlu dikenal pasti dan disahkan bagi menentukan tahap capaian maklumat yang dibenarkan; b) Setiap pengguna sistem perlu diberi peranan mengikut skop dan tanggungjawab yang ditetapkan; dan c) Memastikan pembekal diberi penjelasan dan menandatanganiakuan pematuhan PKS mengenai keperluan mematuhi kontrak dan peraturan keselamatan yang ditetapkan.	Pengurus ICT/ Pentadbir Sistem/ Pembekal
--	--	---

10.1.2 Melindungi Transaksi Perkhidmatan Atas Talian

	a) Maklumat yang terlibat dalam transaksi perkhidmatan atas talian hendaklah dilindungi daripada penghantaran yang tidak lengkap, <i>misrouting</i>, pengubahan mesej yang tidak dibenarkan, pendedahan yang	Pengurus ICT/ Pentadbir Sistem
--	---	---



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

tidak dibenarkan dan duplikasi mesej; dan

- b) Kawalan terhadap keterdedahan perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan.

10.2 Keselamatan Dalam Proses Pembangunan dan Sokongan

Memastikan keselamatan maklumat diwujudkan dan dilaksanakan dalam kitar hayat pembangunan sistem.

10.2.1 Polisi Keselamatan Dalam Pembangunan Sistem

Tatacara pembangunan perisian dan sistem yang mengambil kira aspek keselamatan maklumat hendaklah diwujudkan dan dilaksanakan di dalam organisasi dengan membangunkan Dokumen Pelan Pengurusan Keselamatan Maklumat (ISMP) semasa proses pembangunan sistem.

Pengurus ICT

10.2.2 Prosedur Kawalan Perubahan Sistem

Prosedur kawalan perubahan hendaklah diwujudkan bagi mengawal sebarang perubahan terhadap sistem sepanjang kitar hayat pembangunan sistem.
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:
a) Mengawal pelaksanaan perubahan menggunakan prosedur kawalan

Pengurus ICT/
Pentadbir Sistem/
Pemilik Sistem



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	perubahan yang ditetapkan dan pelaksanaan hanya mengikut keperluan sahaja; b) Perubahan atau pengubahsuaian ke atas perisian dan sistem hendaklah diuji, didokumenkan dan disahkan sebelum diguna pakai; dan c) Setiap perubahan kepada pengoperasian sistem perlu dikaji semula dan diuji untuk memastikan tiada sebarang masalah yang timbul terhadap operasi dan keselamatan maklumat.	
10.2.3 Semakan Teknikal Aplikasi Selepas Perubahan Platform		
	Semakan dan pengujian terhadap aplikasi kritikal 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



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

10.2.4 Kawalan Terhadap Perubahan Kepada Perisian

	Sebarang perubahan terhadap perisian adalah tidak digalakkan, kecuali kepada perubahan yang perlu sahaja dan perubahan tersebut perlu dihadkan.	Pentadbir Sistem
--	---	------------------

10.2.5 Prinsip Kejuruteraan Sistem Yang Selamat

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

10.2.6 Persekitaran Pembangunan Sistem Yang Selamat

	Persekitaran pembangunan sistem yang selamat perlu diwujudkan sepanjang kitar hayat pembangunan sistem. Secara umumnya kitar hayat pembangunan sistem termasuk skop dan objektif sistem, pengumpulan keperluan, reka bentuk, pelaksanaan, ujian, penerimaan, pemasangan, konfigurasi, penyelenggaraan dan pelupusan.	Pentadbir Sistem
--	--	------------------

10.2.7 Pembangunan Sistem Secara Luaran

	Sebarang aktiviti pembangunan sistem yang melibatkan sumber luar perlu dikawal selia dan dipantau. Perkara-perkara yang perlu dipatuhi	Pengurus ICT/ Pentadbir Sistem/ Pembekal
--	--	--



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

adalah termasuk yang berikut:

- a) Memastikan spesifikasi perolehan mengandungi klausa tertentu berhubung keperluan keselamatan, pensijilan keselamatan produk, ketersediaan kod sumber, keperluan pelupusan data, keutamaan terhadap teknologi dan kepakaran tempatan, serta keperluan kompetensi pasukan pembangunan;
- b) Organisasi hendaklah memastikan Intellectual Property Rights (IPR) dan kod sumber menjadi hak milik organisasi;
- c) Memasukkan klausa ke dalam kontrak yang membenarkan jabatan melaksanakan semakan terhadap kod sumber; dan
- d) Memasukkan klausa ke dalam kontrak yang membenarkan jabatan mendapat hak pemilikan kod sumber dan melaksanakan pengolahan risiko.

10.2.8 Ujian Keselamatan Sistem

Aktiviti pengujian penerimaan sistem hendaklah dilaksanakan ke atas sistem baru, naik taraf dan versi baru berdasarkan kriteria yang telah ditetapkan.

Pengurus ICT dan Pentadbir Sistem



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

Bagi memastikan integriti data, pengujian hendaklah dijalankan ke atas tiga (3) peringkat pemprosesan maklumat iaitu peringkat kemasukan data (*input*), peringkat pemprosesan data (*process*) dan peringkat penjaanaan laporan (*output*).

10.2.9 Pengekodan Selamat (*Secure Coding*)

- | | |
|--|-----------------------------------|
| <p>a) Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan mengikut garis panduan semasa yang telah ditetapkan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha</p> <p>b) Prinsip dan prosedur kejuruteraan sistem hendaklah sentiasa dikaji dari semasa ke semasa mengikut keperluan dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat.</p> | <p>ICTSO dan Pentadbir Sistem</p> |
|--|-----------------------------------|

10.3 Data Ujian

Memastikan data yang digunakan untuk pengujian adalah dilindungi.

10.3.1 Perlindungan Data Ujian

Data ujian hendaklah bersesuaian, dilindungi dan dikawal.	Pengurus ICT
--	---------------------



BAB 11: HUBUNGAN DENGAN PEMBEKAL

Objektif: Memastikan aset dilindungi sepenuhnya daripada akses yang tidak sewajarnya oleh pembekal.

Bil	Perkara	Tanggungjawab
11.1 Keselamatan Maklumat dalam Hubungan Pembekal		
11.1.1 Polisi Keselamatan Maklumat ke atas Pembekal		
	Semua pembekal adalah tertakluk kepada Dasar Keselamatan Kerajaan yang berkuat kuasa. Perkara perkara yang perlu dipatuhi adalah seperti berikut: a) Pembekal hendaklah menandatangani Surat Akuan Pematuhan PKS Jabatan; b) Pembekal hendaklah menandatangani Akuan Akta Rahsia Rasmi 1972; c) Pembekal hendaklah menjalani ujian tapisan keselamatan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO); dan d) Pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas.	ICTSO/ Pembekal



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

11.1.2 Kawalan Keselamatan Maklumat Melalui Perjanjian dengan Pembekal

	Perjanjian dengan pihak pembekal hendaklah merangkumi keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan perkhidmatan teknologi maklumat dan komunikasi.	CDO, Pengurus ICT dan Pembekal
--	---	--------------------------------

11.1.3 Kawalan Keselamatan Maklumat Dengan Pembekal dan Pihak Ketiga

	Perjanjian dengan pembekal hendaklah meliputi risiko keselamatan yang merangkumi perkhidmatan ICT dan kesinambungan bekalan produk dengan pihak ketiga.	ICTSO, Pengurus ICT, Pembekal
--	---	-------------------------------------

11.2 Pengurusan Penyampaian Perkhidmatan Pembekal

11.2.1 Pemantauan dan Penilaian Perkhidmatan Pembekal

	Jabatan hendaklah memantau, menyemak dan mengaudit perkhidmatan pembekal secara berkala.	Pentadbir Sistem
--	--	------------------

11.2.2 Pengurusan Perubahan Perkhidmatan Pembekal

	Setiap perubahan perkhidmatan pembekal hendaklah dilaksanakan secara teratur dan mengikut SOP yang ditetapkan. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a) Perubahan di dalam perjanjian bersama pembekal;	Pengurus ICT
--	---	--------------



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- b) Perubahan yang dilakukan oleh jabatan 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, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.

11.3 Keselamatan Maklumat Dalam Pengurusan Projek

11.3.1 Pengurusan Projek

Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh Pihak Ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut:

- a) Risiko keselamatan maklumat hendaklah dinilai dan diambil kira di peringkat awal bagi sesuatu projek;
- b) Keperluan keselamatan maklumat perlu ditangani pada peringkat awal pelaksanaan projek;
- c) Mengambil kira risiko dalaman dan luaran keselamatan maklumat semasa pelaksanaan projek;
- d) Semakan dan keberkesanan pelaksanaan penguraian

- i. Pengurus ICT/Ketua Seksyen
 - ii. ICTSO
 - iii. Pengurus Projek
- Pasukan Projek



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

risiko keselamatan maklumat hendaklah diuji dan dinilai.

11.3.2 Keselamatan Maklumat Dalam Pengurusan Projek

Perkara yang perlu dipatuhi adalah seperti berikut:

- a) Mengenal pasti maklumat yang terlibat selari dengan keperluan keselamatan Kementerian dan berpotensi memberikan impak negatif;
- b) Perlindungan perlu mengambil kira kerahsiaan, integriti dan ketersediaan;
- c) Memastikan jaminan keselamatan maklumat berkaitan identiti pihak ketiga dilaksanakan dan disahkan;
- d) Memastikan kawalan akses kepada pihak ketiga;
- e) Memaklumkan kepada pengguna tentang tugas dan tanggungjawab mereka;
- f) Melaksanakan pemantauan ke atas log transaksi dan kebocoran maklumat oleh pihak ketiga;
- g) Pematuhan kepada undang-undang dan peraturan yang berkuat kuasa;
- h) Memastikan klausa keselamatan maklumat yang berkaitan diambil kira di dalam perjanjian atau kontrak;
- i) Mengenal pasti risiko keselamatan

- i. Pengurus ICT/
Ketua Seksyen
- ii. ICTSO
Pengurus Projek/
Pasukan Projek



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;

- j) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga;
- k) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem maklumat hendaklah mengambil kira kawalan keselamatan;
- l) Sistem maklumat yang dibangunkan sama ada secara dalaman atau luaran hendaklah dikaji supaya mengikut keperluan pengguna dan selaras dengan dasar atau peraturan berkaitan yang berkuat kuasa;
- m) Sistem maklumat yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan; dan
- n) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan

	JKPTG-ISMS-P1-001 POLISI KESELAMATAN SIBER	
	keselamatan.	



BAB 12: PENGURUSAN INSIDEN KESELAMATAN ICT

Objektif: Memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, tepat dan berkesan bagi memastikan perkhidmatan ICT organisasi dapat beroperasi semula.

Bil	Perkara	Tanggungjawab
12.1 Pengurusan Insiden Dan Penambahbaikan Keselamatan Maklumat		
12.1.1 Tanggungjawab Dan Prosedur		
	Prosedur bagi mengurus insiden keselamatan ICT perlu diwujudkan dan didokumenkan. Jabatan bertanggungjawab dalam pengurusan pengendalian insiden keselamatan ICT.	Pasukan CSIRT
12.1.2 Pelaporan Insiden Keselamatan Maklumat		
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada Pasukan CSIRT. Semua maklumat adalah SULIT dan tidak boleh didedahkan tanpa kebenaran daripada ICTSO; b) Mematuhi prosedur operasi standard (SOP) keselamatan ICT Jabatan; c) Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan,	Pasukan CSIRT/ CERT/ GCERT
Versi: 2.0		Muka Surat: 106



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; d) Menyimpan jejak audit dan memelihara bahan bukti; dan e) Menyediakan dan melaksanakan plan tindakan pemulihan.	
--	--	--

12.1.3 Pelaporan Kelemahan Keselamatan Maklumat

	Insiden keselamatan siber adalah meliputi perkara perkara berikut: a) Pelanggaran Polisi (<i>Violation of Policy</i>) Penggunaan aset ICT bagi tujuan kebocoran maklumat dan/ atau mencapai maklumat yang melanggar Polisi Keselamatan Siber. b) Penghalangan Penyampaian Perkhidmatan (<i>Denial of Service</i>) Ancaman ke atas keselamatan sistem komputer di mana perkhidmatan pemprosesan maklumat sengaja dinafikan terhadap pengguna sistem. Ia melibatkan sebarang tindakan yang menghalang sistem daripada berfungsi secara normal. Termasuk <i>denial of service</i> (DoS), <i>distributed denial of service</i> (DDoS) dan <i>sabotage</i>. c) Pencerobohan (<i>Intrusion</i>)	Pasukan CSIRT/ CERT/ GCERT
--	--	-----------------------------------



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

Mengguna dan mengubahsuai ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak. Ia termasuk capaian tanpa kebenaran, pencerobohan laman web, melakukan kerosakan kepada sistem (*system tampering*), pindaan data (*modification of data*) dan pindaan kepada konfigurasi sistem.

d) Pemalsuan (*Forgery*)

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

e) Spam

Spam adalah e-mel yang dihantar ke akaun e-mel orang lain yang tidak dikenali penghantar dalam satu masa dan secara berulang kali (kandungan e mel yang sama). Ini menyebabkan kesesakan rangkaian dan tindak balas menjadi perlahan.

f) Malicious Code

Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, <i>trojan horse</i>, <i>worm</i>, <i>spyware</i> dan sebagainya. g) <i>Harrassment/ Threats</i> Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atasebab tertentu. h) <i>Attempts/ Hack Threats/ Information Gathering</i> Percubaaan (sama ada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran. Termasuk <i>spoofing</i>, <i>phishing</i>, <i>probing</i>, <i>war driving</i> dan <i>scanning</i>. i) <i>Kehilangan Fizikal (Physical Loss)</i> Kehilangan capaian dan kegunaan disebabkan kerosakan, kecurian dan kebakaran ke atas aset ICT berpunca dari ancaman pencerobohan.	
--	--	--

12.1.4 Penilaian dan Keputusan Insiden Keselamatan Maklumat

	Agensi hendaklah menilai sama ada serangan diklasifikasikan sebagai insiden. Menentukan Keutamaan Tindakan Ke Atas Insiden Tindakan ke atas insiden yang dilaporkan akan dibuat berasaskan tahap kritikal sesuatu insiden. Keutamaan akan ditentukan seperti berikut:	Pasukan CSIRT/ CERT/ GCERT
--	---	-----------------------------------



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

a) Keutamaan 1:

Aktiviti yang berkemungkinan mengancam nyawa atau keselamatan negara.

b) Keutamaan 2:

- i. Pencerobohan atau percubaan menceroboh melalui infrastruktur internet ke atas peralatan rangkaian;
- ii. Penyebaran penafian penyampaian perkhidmatan (*distributed denial of service*);
- iii. Serangan atau pendedahan keterdedahan terbaru (*new vulnerabilities*); atau
- iv. Lain-lain insiden seperti:
 - Pencerobohan melalui pemalsuan identiti;
 - Pengubahsuaian laman web, perisian, atau mana-mana komponen sistem tanpa pengetahuan, arahan atau persetujuan pihak yang berkenaan; dan
 - Gangguan sistem untuk pemprosesan data atau penyimpanan data tanpa kebenaran.

12.2 Pelantikan Pegawai Bertanggungjawab

Pegawai Keselamatan ICT (ICTSO) dan anggota Pasukan CSIRT hendaklah dilantik secara rasmi oleh Ketua Jabatan dan dimaklumkan kepada warga Jabatan.

KJ/ CDO



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

Insiden keselamatan siber yang melibatkan Maklumat Rahsia Rasmi hendaklah dirujuk kepada CGSO untuk tindakan selanjutnya.

12.3 Pengumpulan dan Pengendalian Bukti

Maklumat mengenai insiden keselamatan ICT perlu dikumpul, dianalisis dan disimpan oleh Pengurus ICT bagi tujuan perancangan dan tindakan untuk melaksanakan peningkatan dan kawalan tambahan.

Pasukan CSIRT hendaklah memastikan bahan bukti berkaitan insiden keselamatan ICT dapat disediakan, disimpan, disenggarakan dan mempunyai perlindungan keselamatan. Penyediaan bahan bukti seperti jejak audit, *backup* berkala dan *off-site backup* hendaklah mengikut tatacara pengendalian yang berkuat kuasa.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Melindungi integriti bahan bukti;
- b) Mengumpul dan menyimpan bahan bukti bagi tujuan analisis;
- c) Merekodkan semua maklumat insiden termasuk maklumat pegawai yang terlibat, perisian, perkakasan dan peralatan yang digunakan;
- d) Memaklumkan kepada pihak berkuasa perundangan seperti

Pengurus ICT



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

	pegawai undang undang dan polis (jika perlu); e) Mendapatkan nasihat dari pihak berkuasa perundangan ke atas bahan bukti yang diperlukan (jika perlu); dan f) Menyediakan laporan insiden kepada CDO.	
--	--	--



BAB 13: PENGURUSAN KESINAMBUNGAN PERKHIDMATAN (PKP) (BUSINESS CONTINUITY MANAGEMENT (BCM))

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

Bil	Perkara
13.1 Kesenambungan Perkhidmatan	
	Ketua Jabatan bertanggungjawab memastikan perkhidmatan tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.
13.2 Pelan Kesenambungan Perkhidmatan (<i>Business Continuity Plan</i> (BCP))	
	CDO hendaklah membangunkan Pelan Kesenambungan Perkhidmatan untuk mengekalkan kesinambungan perkhidmatan bagi memastikan tiada gangguan di dalam penyediaan perkhidmatan agensi. Pelan ini mestilah diperakui oleh pihak pengurusan Jabatan dan perkara-perkara berikut perlu diberi perhatian: a) Melantik ahli Pasukan Pemulihan Bencana; b) Mengenal pasti dan mendokumenkan semua tanggungjawab dan prosedur kecemasan atau pemulihan; c) Melaksanakan prosedur-prosedur kecemasan dan simulasi pemulihan bencana bagi memastikan pemulihan dapat dilakukan dalam jangka masa yang telah ditetapkan seperti yang tertakluk dalam pelan pemulihan bencana; d) Mengadakan program kesedaran dan latihan kepada pengguna mengenai prosedur kecemasan; e) Mengkaji dan mengemas kini pelan sekurang-kurangnya setahun sekali;



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- f) Membuat *backup*; dan
- g) Mewujudkan Pusat Pemulihan Bencana di lokasi lain.

13.3 Perubahan atau Pengecualian PKP

Sekiranya terdapat perubahan/ pengemaskinian atau pengecualian yang perlu dilakukan, permintaan secara bertulis termasuk keterangan dan kebenaran untuk pengecualian/ perubahan hendaklah dikemukakan kepada Ketua Jabatan.

13.4 Program Latihan dan Kesedaran Terhadap PKP

Semua kakitangan perlu mempunyai kesedaran dan mengetahui peranan masing-masing terhadap PKP. KJ/ KB bertanggungjawab dalam memastikan latihan dan program kesedaran terhadap PKP dilaksanakan setiap tahun.

13.5 Pengujian PKP

CDO perlu memastikan perkara-perkara berikut:

- a) PKP perlu diuji dua (2) tahun sekali atau selepas perubahan utama, atau yang mana terdahulu bagi memastikan semua pihak yang berkenaan mengetahui dan maklum akan pelaksanaannya;
- b) Salinan PKP mestilah disimpan di lokasi berasingan bagi mengelakkan kerosakan akibat bencana di lokasi utama. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan;
- c) Ujian PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan;



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- d) Jabatan hendaklah memastikan salinan Pelan Kesyinambungan Perkhidmatan sentiasa dikemas kini dan dilindungi seperti di lokasi utama; dan
- e) Komponen PKP seperti Pelan Pemulihan Bencana (Disaster Recovery Plan – DRP), Pelan Komunikasi Krisis (Crisis Communication Plan – CCP) dan Pelan Tindak Balas Kecemasan (Emergency Response Plan – ERP) perlu diuji dua (2) tahun sekali atau selepas perubahan utama, atau yang mana terdahulu.

13.6 Ketersediaan Kemudahan Pemprosesan Maklumat

Semua sistem aplikasi dan perkakasan yang kritikal hendaklah mempunyai kemudahan redundancy dan diuji (*failover test*) keberkesanannya mengikut keperluan.



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

BAB 14: PEMATUHAN

Objektif: Untuk menghindar pelanggaran undang-undang jenayah dan sivil, perlembagaan, peraturan atau ikatan kontrak dan sebarang keperluan keselamatan lain.

Bil	Perkara
14.1 Pematuhan Polisi	
	Adalah menjadi tanggungjawab Ketua Jabatan untuk memastikan bahawa pematuhan dan sebarang pelanggaran dielakkan. Langkah-langkah perlu bagi mengelakkan sebarang pelanggaran perundangan termasuklah memastikan setiap pengguna membaca, memahami dan mematuhi Polisi Keselamatan Siber Jabatan dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.
14.2 Keperluan Perundangan	
	Kakitangan Jabatan perlu memastikan senarai perundangan dan peraturan yang berkuat kuasa dari semasa ke semasa perlu dipatuhi oleh semua kakitangan di Jabatan adalah seperti di LAMPIRAN C.
14.3 Perlindungan dan Privasi Data Peribadi	
	Kakitangan perlu sedar bahawa data kegunaan peribadi yang dijana dalam aset ICT adalah milik jabatan. Pihak pengurusan tidak menjamin kerahsiaan data peribadi yang disimpan dalam aset ICT. Untuk tujuan keselamatan dan penyelenggaraan rangkaian, pegawai yang diberi kuasa perlu mengawasi peralatan, sistem dan rangkaian. Pihak pengurusan berhak mengaudit rangkaian dan sistem secara berkala bagi memastikan ia mematuhi PKS.
Versi: 2.0	Muka Surat: 116



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

Pihak pengurusan perlu menggalakkan dasar privasi yang adil dan bertanggungjawab bagi memastikan semua maklumat peribadi digunakan berdasarkan keperluan untuk mengelakkan penyalahgunaan maklumat.

Pendedahan maklumat peribadi tentang kakitangan jabatan kepada pihak ketiga tidak sepatutnya berlaku kecuali:

- a) Dikehendaki oleh undang-undang atau peraturan;
- b) Dengan persetujuan yang jelas dan nyata daripada kakitangan tersebut; atau
- c) Setelah menerima persetujuan bertulis daripada pihak ketiga di mana maklumat akan dilindungi dengan tahap keselamatan dan privasi yang mencukupi seperti yang ditentukan oleh Unit Undang-undang serta perjanjian jelas diperoleh daripada pengurusan sumber manusia; dan
- d) Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian dan pengeluaran yang tidak sah mengikut undang-undang, peraturan, kontrak dan keperluan jabatan.

14.4 Semakan Keselamatan Maklumat

Semakan keselamatan maklumat mestilah diambil kira seperti berikut:

- a) Pematuhan pemeriksaan ke atas PKS, piawaian dan prosedur perlu dilakukan secara tahunan. Pemeriksaan ini mestilah melibatkan usaha bagi menentukan kawalan yang mencukupi dan dipatuhi;
- b) Pengauditan perlu dilaksanakan sekurang-kurangnya sekali setahun terhadap pengoperasian sistem maklumat bagi meminimalkan ancaman dan meningkatkan ketersediaan sistem; dan
- c) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.

14.5 Pelanggaran Perundangan

Mengambil tindakan tatatertib ke atas sesiapa yang terlibat di dalam semua perbuatan kecuai, kelalaian dan pelanggaran keselamatan termasuk Polisi Keselamatan Siber yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972. Antara tindakan yang boleh diambil terhadap pihak ketiga adalah penamatan kontrak.

14.6 Akuan Pematuhan Polisi Keselamatan Siber

Ketua Jabatan adalah bertanggungjawab untuk memastikan setiap pegawai menandatangani Akuan Pematuhan Polisi Keselamatan Siber seperti di **LAMPIRAN A**.

14.7 Pematuhan Terhadap Hak Harta Intelek (Intellectual Property Rights)

Prosedur pengawalan hendaklah dilaksanakan bagi memastikan pematuhan kepada perundangan, peraturan dan keperluan kontrak berkaitan produk yang mempunyai IPR termasuk perisian proprietary.



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

Bab 15: Risikan Ancaman (Threat Intelligence)

Objektif: Memberi kesedaran tentang persekitaran ancaman organisasi supaya tindakan mitigasi yang sewajarnya dapat diambil.

Bil	Perkara	Tanggungjawab
15.1 Keperluan Risikan Ancaman		
	Maklumat mengenai ancaman sedia ada atau baharu hendaklah dikumpulkan daripada sumber luaran dan dalaman, dan dianalisis untuk: a) Memudahkan tindakan sewajarnya diambil untuk mencegah ancaman daripada menyebabkan kemudaratan kepada organisasi; b) Mengurangkan kesan ancaman tersebut. Aktiviti perisikan ancaman hendaklah termasuk: a) Mengenal pasti, memeriksa dan memilih sumber maklumat dalaman dan luaran yang diperlukan dan sesuai untuk melaksanakan tindakan yang diperlukan berdasarkan pengeluaran perisikan ancaman; b) Memproses dan menganalisis maklumat untuk memahami bagaimana ia berkaitan dan bermakna kepada organisasi;	ICTSO dan CSIRT JKPTG



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- c) Berkomunikasi dan berkongsi kepada individu yang berkaitan dalam format yang boleh difahami.

Perisikan ancaman hendaklah dianalisis dan kemudian digunakan:

- a) Dengan melaksanakan proses untuk memasukkan maklumat yang dikumpulkan dari sumber perisikan ancaman ke dalam proses pengurusan risiko keselamatan maklumat organisasi;
- b) Sebagai input tambahan kepada kawalan pencegahan dan pengesanan teknikal seperti firewall, intrusion detection system, atau penyelesaian anti perisian hasad;
- c) Sebagai input kepada proses dan teknik Penilaian Tahap Keselamatan.



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

KAKITANGAN JABATAN

LAMPIRAN A (I)



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

LAMPIRAN A (I)



AKUAN PEMATUHAN POLISI KESELAMATAN SIBER
JABATAN KETUA PENGARAH TANAH DAN GALIAN
PERSEKUTUAN

Nama (HURUF BESAR) :

No. Kad Pengenalan :

Jawatan :

Bahagian :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

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

Tandatangan :

Tarikh :

Pengesahan Pegawai Keselamatan ICT

.....

(Tandatangan & Cap Jawatan)

Jabatan Ketua Pengarah Tanah dan Galian Persekutuan

Tarikh:

* Polisi Keselamatan Siber boleh dicapai menerusi <http://www.jkptg.gov.my>



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

PEMBEKAL/ PIHAK KETIGA
LAMPIRAN A (II), B (I) & B (II)



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

LAMPIRAN A (II)



AKUAN PEMATUHAN POLISI KESELAMATAN SIBER
JABATAN KETUA PENGARAH TANAH DAN GALIAN
PERSEKUTUAN

Nama (HURUF BESAR) :

No. Kad Pengenalan :

Nama Syarikat :

No. Pendaftaran Syarikat:

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

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

Tandatangan :

Tarikh :

Pengesahan Pegawai Keselamatan ICT

.....

(Tandatangan & Cap Jawatan)

Jabatan Ketua Pengarah Tanah dan Galian Persekutuan

Tarikh:

* Polisi Keselamatan Siber boleh dicapai menerusi <http://www.jkptg.gov.my>



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

LAMPIRAN B (I)

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

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

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

Tandatangan :
Nama (huruf besar) :
No. Kad Pengenalan :
Jawatan :
Jabatan / Organisasi :
Tarikh :
Disaksikan Oleh :

(Tandatangan)

Nama (huruf besar) :
No. Kad Pengenalan :
Jawatan :
Jabatan / Organisasi :
Tarikh :
Cap Jabatan / Organisasi :



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

LAMPIRAN B (II)

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

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

Dengan ini menjadi satu kesalahan di bawah Akta tersebut bagi saya menyampaikan dengan tiada kebenaran apa-apa rahsia rasmi atau suratan rasmi kepada mana-mana orang lain, sama ada atau tidak orang itu memegang jawatan dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau mana-mana Kerajaan Malaysia, dan sama ada di Malaysia atau di negara luar, sebelum dan selepas saya tamat kontrak perkhidmatan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia.

Saya mengaku bahawa tidak lagi ada dalam milik saya atau kawalan saya apa-apa perkataan kod rasmi, isyarat timbal, atau kata laluan rasmi yang rahsia, atau apa-apa benda, suratan atau maklumat, anak kunci, rencana, alat meteri, atau cap bagi atau yang dipunyai, atau diguna, dibuat atau diadakan oleh mana-mana jabatan Kerajaan atau oleh mana-mana pihak berkuasa diplomat yang dilantik oleh atau yang bertindak di bawah kuasa Kerajaan Malaysia atau Seri Paduka Baginda yang tidak dibenarkan berada dalam milikan atau kawalan saya.

Tandatangan	:	
Nama (huruf besar)	:	
No. Kad Pengenalan	:	
Jawatan	:	
Jabatan / Organisasi	:	
Tarikh	:	
Disaksikan Oleh	:	
		(Tandatangan)
Nama (huruf besar)	:	
No. Kad Pengenalan	:	
Jawatan	:	
Jabatan / Organisasi	:	
Tarikh	:	
Cap Jabatan / Organisasi	:	



RUJUKAN

SENARAI PERUNDANGAN DAN PERATURAN

Senarai perundangan dan peraturan yang terpakai adalah seperti berikut tetapi tidak terhad kepada:

1. Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024
2. Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024
3. Pekeliling Am Bilangan 4 Tahun 2022 : Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam – 1 Ogos 2022.
4. Arahan Keselamatan (Semakan dan Pindaan 2017).
5. Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan.
6. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002.
7. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan.
8. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.
9. 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.
10. Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007.



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

11. Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007.
12. Surat Pekeliling Perbendaharaan Bil. 3/1995 – Peraturan Perolehan Perkhidmatan Perundingan.
13. Akta Tandatangan Digital 1997.
14. Akta Rahsia Rasmi 1972.
15. Akta Jenayah Komputer 1997.
16. Akta Hak Cipta (Pindaan) Tahun 1997.
17. Akta Komunikasi dan Multimedia 1998.
18. Perintah - Perintah Am.
19. Arahan Perbendaharaan.
20. Arahan Teknologi Maklumat 2007.
21. Garis Panduan Keselamatan MAMPU 2004.
22. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009.
23. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesyntambungan Perkhidmatan.
24. Arahan Teknologi Maklumat dan Akta Aktiviti Kerajaan Elektronik (Akta 680) (Tahun 2007).
25. Pekeliling Am Bil. 1 Tahun 2009 – Manual Pengurusan Aset Menyeluruh Kerajaan.
26. Surat Pekeliling Am Bilangan 1 Tahun 2009 Garis Panduan Mengenai Tatacara Memohon Kelulusan Teknikal Projek ICT Agensi Kerajaan.
27. Surat Arahan Ketua Setiausaha Negara – Langkah-langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit Atau Lain-lain Peralatan Komunikasi ICT Tanpa Kebenaran (Tarikh : 31 Januari 2007).
28. Surat Arahan Ketua Pengarah MAMPU – Amalan Terbaik Penggunaan Media Jaringan Sosial (Tarikh : 8 April 2011).



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

29. Surat Arahan Ketua Pengarah MAMPU – Pemantapan Penggunaan Dan Pengurusan E-Mel (Tarikh : 1 Julai 2010).
30. Surat Arahan Ketua Pengarah MAMPU – Panduan Pelaksanaan Pengurusan Projek ICT Sektor Awam (5 Mac 2010).
31. Surat Arahan Ketua Pengarah MAMPU – Garis Panduan Transisi Protokol Internet Versi 6 (IPV6) Sektor Awam (Tarikh : 4 Januari 2010).
32. Surat Arahan Ketua Pengarah MAMPU – Penggunaan Media Jaringan Sosial Di Sektor Awam (Tarikh : 19 November 2009).
33. Surat Arahan Ketua Pengarah MAMPU – Penggunaan Smartphone, Personel Digital Assistant Dan Alat Komunikasi Mudah Alih Sebagai Saluran Komunikasi Tambahan (Tarikh : 15 September 2009).
34. Garis Panduan Penggunaan ICT Ke Arah ICT Hijau Dalam Perkhidmatan Awam (Ogos 2010).
35. Arahan Teknologi Maklumat Dan Akta Aktiviti Kerajaan Elektronik (Akta 680) (Tahun 2007).
36. Garis Panduan IT Outsourcing (Oktober 2006).
37. Garis Panduan Penyimpanan dan Pemeliharaan Rekod Elektronik Sektor Awam.
38. Arahan 20 (Semakan Semula) – Dasar dan Mekanisme Pengurusan Bencana Negara.
39. Arahan 24 - Dasar Dan Mekanisme Pengurusan Krisis Siber Negara.
40. Pekeliling Am Bil. 1 Tahun 2015 – Pelaksanaan Data Terbuka Sektor Awam.
41. Rancangan Malaysia Ke-11.
42. Panduan Pelaksanaan Audit Dalam ISMS Sektor Awam.
43. Surat Arahan Ketua Pengarah MAMPU Pelaksanaan dan Penggunaan Aplikasi Digital Document Management System (DDMS) Sektor Awam 25 Januari 2015.
44. Dasar Kriptografi Negara 12 Julai 2013.
45. Surat Pekeliling Perbendaharaan – Garis Panduan Mengenai Pengurusan Perolehan Information Telecommunication Technology ICT Kerajaan SPP 3/2013.



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

46. Pekeliling Perbendaharaan Malaysia PK 2/2013 – Kaedah Perolehan Kerajaan.
47. Garis Panduan Perolehan ICT Kerajaan Kementerian Kewangan Malaysia. Cabutan Pekeliling Perbendaharaan Malaysia PK 2.2/2013.
48. Arahan Ketua Pegawai Keselamatan Kerajaan 5 Jun 2012 – Langkah-langkah Keselamatan Perlindungan Bagi Mencegah Kehilangan Komputer Riba Dan Peranti Mudah Alih Di Sektor Awam.
49. PK3.2 - Manual Perolehan Perkhidmatan Perunding Edisi 2011 (Pindaan Kedua).
50. Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat 24 November 2010.
51. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesenambungan Perkhidmatan Agensi Sektor Awam, 22 Januari 2010.
52. Akta 709 – Akta Perlindungan Data Peribadi 2010.
53. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan, 23 November 2007.
54. Arahan Ketua Setiausaha Negara Bil. 1 Tahun 2007 – Langkah-langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit Atau Lain-lain Peralatan Komunikasi ICT Tanpa Kebenaran Atau Kuasa Yang Sah Di Agensi-agensi Kerajaan.
55. Surat Arahan Ketua Setiausaha Negara - Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) Di Agensi-agensi Kerajaan, 20 Oktober 2006.
56. Akta 658 – Akta Perdagangan Elektronik 2006.
57. Akta 629 – Akta Arkib Negara 2003.
58. Akta 606 – Akta Cakera Optik 2000.
59. Surat Pekeliling Am Bilangan 2/1987 – Peraturan Pengurusan Rahsia Rasmi selaras Dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987).
60. Akta 298 – Kawasan Larangan Tempat Larangan 1959.
61. Akta 56 – Akta Keterangan 1950.



JKPTG-ISMS-P1-001
POLISI KESELAMATAN SIBER

- 62. National Cyber Security Policy (NCSP).
- 63. Guideline to Determine Information Security Professionals Requirement for the CNII Agencies/ Organisations.
- 64. Arahan Tetap Sasaran Penting.
- 65. Garis Panduan Pengurusan Rekod Elektronik oleh Jabatan Arkib Negara.
- 66. Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi.
- 67. Perintah Am Bab D.
- 68. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSA) versi 1.0 April 2016; dan

Semua Perundangan semasa yang terpakai keatas JKPTG.