KPT.100-1/3/1 JLD2 (7)

KEMENTERIAN PENDIDIKAN TINGGI

ARAHAN PENTADBIRAN KETUA SETIAUSAHA

BIL. 1 TAHUN 2026

POLISI KESELAMATAN SIBER

KEMENTERIAN PENDIDIKAN TINGGI

TUJUAN

1. Arahan Pentadbiran ini bertujuan untuk memaklumkan penguatkuasaan Polisi Keselamatan Siber Kementerian Pendidikan Tinggi (PKS KPT) Versi 3.0 yang menggantikan PKS KPT Versi 2.0, di samping menjelaskan keperluan pematuhan polisi tersebut oleh warga KPT, pembekal dan pihak ketiga yang berurusan dengan KPT bagi memastikan keselamatan dan perlindungan maklumat, sistem, perkhidmatan serta aset siber Kementerian.

LATAR BELAKANG

2. Perkembangan teknologi dan pendigitalan perkhidmatan Kerajaan telah meningkatkan kebergantungan KPT kepada sistem, aplikasi, rangkaian dan perkhidmatan digital dalam melaksanakan fungsi dan menyampaikan perkhidmatan Kementerian. Pada masa yang sama, perkembangan ini turut meningkatkan pendedahan kepada ancaman keselamatan siber seperti perisian hasad (*malware*), serangan penafian perkhidmatan teragih (*Distributed Denial-of-Service* – DDoS), pencerobohan data dan penipuan siber yang boleh menjejaskan kerahsiaan, integriti dan ketersediaan maklumat serta kesinambungan penyampaian perkhidmatan KPT.

3. Sehubungan dengan itu, KPT telah membangunkan PKS KPT sebagai dasar utama yang menetapkan prinsip, tadbir urus, peranan, tanggungjawab dan kawalan keselamatan siber yang perlu dilaksanakan oleh warga KPT serta pihak yang berkaitan bagi memastikan aset maklumat dan aset siber Kementerian dilindungi dengan sewajarnya.

4. PKS KPT Versi 2.0 telah dikuatkuasakan melalui Arahan Pentadbiran Ketua Setiausaha Bil. 1 Tahun 2025. Bagi memastikan polisi tersebut kekal relevan dengan perkembangan landskap keselamatan siber, keperluan perundangan dan kawal selia serta keperluan semasa Kerajaan, semakan dan pengemaskinian terhadap PKS KPT Versi 2.0 telah dilaksanakan. Semakan tersebut termasuklah penjajaran PKS KPT Versi 2.0 dengan Tataamalan Keselamatan Siber Jabatan Digital Negara (JDN) Versi 1.3. Hasil daripada

semakan dan penjajaran tersebut, PKS KPT Versi 3.0 telah dibangunkan bagi memperkukuh tadbir urus, kawalan dan pengurusan keselamatan siber Kementerian serta memastikan keperluan keselamatan siber semasa dan tanggungjawab KPT sebagai Entiti Infrastruktur Maklumat Kritikal Negara (NCII) dilaksanakan dengan sewajarnya.

5. PKS KPT Versi 3.0 turut mengambil kira keperluan standard ISO/IEC 27001:2022 Sistem Pengurusan Keselamatan Maklumat (*Information Security Management Systems* – ISMS) serta perundangan, arahan, dasar, pekeliling dan garis panduan keselamatan siber Kerajaan yang berkaitan dan berkuat kuasa.

POLISI KESELAMATAN SIBER

6. PKS KPT Versi 3.0 seperti di **Lampiran A** hendaklah dijadikan rujukan dan dipatuhi oleh semua pihak yang tertakluk kepada pemakaian polisi tersebut.

7. PKS KPT Versi 3.0 merangkumi aspek tadbir urus dan pengurusan keselamatan siber yang berkaitan dengan pengurusan, pembangunan, penyelenggaraan, penyediaan, capaian, pemprosesan, penghantaran, perkongsian, penyimpanan dan penggunaan maklumat serta aset siber KPT.

8. Semua warga KPT, pembekal dan pihak ketiga yang diberikan akses kepada maklumat, sistem, aplikasi, rangkaian, kemudahan atau aset siber KPT hendaklah mematuhi kawalan dan keperluan keselamatan yang ditetapkan dalam PKS KPT Versi 3.0 serta peraturan dan prosedur lain yang berkaitan dan berkuat kuasa.

TANGGUNGJAWAB BAHAGIAN DAN AGENSI DI BAWAH KPT

9. Semua Bahagian dan Agensi di bawah KPT hendaklah mematuhi serta menerapkan keperluan PKS KPT Versi 3.0 dalam penyampaian perkhidmatan masing-masing, di samping memastikan warga KPT, pembekal, dan pihak

ketiga di bawah seliaan turut memahami serta mematuhi polisi tersebut. Selain itu, kawalan keselamatan siber hendaklah dilaksanakan berdasarkan tahap risiko aset, setiap insiden wajib dilaporkan serta dikendalikan mengikut prosedur berkuat kuasa, dan kerjasama penuh hendaklah diberikan bagi tujuan pemantauan, penilaian risiko, audit, pematuhan, serta penambahbaikan keselamatan siber Kementerian.

TANGGUNGJAWAB PEMBEKAL DAN PIHAK KETIGA

10. Semua pembekal dan pihak ketiga yang diberikan akses kepada maklumat, sistem, rangkaian, atau kemudahan ICT KPT hendaklah mematuhi PKS KPT Versi 3.0 serta keperluan keselamatan siber Kementerian sepanjang tempoh perkhidmatan. Bagi tujuan tersebut, Bahagian atau Agensi yang berkaitan hendaklah memastikan keperluan keselamatan siber dinyatakan dan dikuatkuasakan melalui kontrak, perjanjian, akuan kerahsiaan, atau instrumen lain yang bersesuaian.

PEMANTAUAN DAN PEMATUHAN

11. Tahap pematuhan terhadap PKS KPT Versi 3.0 hendaklah dipantau secara berterusan melalui mekanisme tadbir urus, pengurusan risiko, pemantauan keselamatan, penilaian pematuhan dan audit yang berkaitan.

12. Sebarang ketidakpatuhan terhadap PKS KPT Versi 3.0 hendaklah ditangani dan diambil tindakan mengikut peraturan dan tatacara yang berkuat kuasa.

TARIKH KUAT KUASA

13. Arahan Pentadbiran Ketua Setiausaha Bil. 1 Tahun 2026 – Polisi Keselamatan Siber Kementerian Pendidikan Tinggi Versi 3.0 ini berkuat kuasa mulai tarikh dikeluarkan.

PEMBATALAN

14. Dengan berkuat kuasanya Arahan Pentadbiran Ketua Setiausaha Bil. 1 Tahun 2026 – Polisi Keselamatan Siber Kementerian Pendidikan Tinggi Versi 3.0 ini, Arahan Pentadbiran Ketua Setiausaha Bil. 1 Tahun 2025 – Polisi Keselamatan Siber Kementerian Pendidikan Tinggi Versi 2.0 adalah dibatalkan.

PEMAKAIAN

15. Arahan Pentadbiran ini terpakai bagi semua Bahagian dan Agensi di bawah KPT kecuali Agensi Kelayakan Malaysia (MQA), Perbadanan Tabung Pendidikan Tinggi Nasional (PTPTN) dan Universiti Awam. PKS KPT Versi 3.0 boleh diakses melalui portal KPT. https://www.mohe.gov.my

Sekian, terima kasih.

"MALAYSIA MADANI"

"BERKHIDMAT UNTUK NEGARA"

Saya yang menjalankan amanah,

.....

(DATUK TS. DR. HJ. AMINUDDIN BIN HASSIM)
Ketua Setiausaha
Kementerian Pendidikan Tinggi
20 November 2026

KEMENTERIAN PENDIDIKAN TINGGI

KEMENTERIAN PENDIDIKAN TINGGI

POLISI KESELAMATAN SIBER

VERSI 3.0

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUAT KUASA
20 Mei 2021	1.0	JPICT Bil. 3 Tahun 2021	29 Oktober 2021
19 Februari 2025	2.0	JPICT Bil. 1 Tahun 2025	26 Februari 2025
3 November 2026	3.0	JPICT Bil. 5 Tahun 2026	

KANDUNGAN

1.0 PENGENALAN 8
1.1 OBJEKTIF 8
1.2 SKOP 9
1.3 PERANAN DAN TANGGUNGJAWAB 9
1.4 PEMAKAIAN 9
1.5 PENGUATKUASAAN DAN SEMAKAN 9
1.6 PERINGATAN PENTING 10
1.7 RUJUKAN 10
1.8 PERTANYAAN 11
2.0 GLOSARI / TERMA RUJUKAN 13
2.1 GLOSARI 13
2.2 TERMA RUJUKAN 14
3.0 KESELAMATAN MAKLUMAT DAN PENGURUSAN MAKLUMAT 20
3.1 TAKRIF KESELAMATAN MAKLUMAT DAN PENGURUSAN MAKLUMAT: 20
3.2 PRINSIP-PRINSIP KESELAMATAN MAKLUMAT 20
3.3 CIRI-CIRI KESELAMATAN MAKLUMAT 22
3.4 KATEGORI MAKLUMAT 22
4.0 PENGURUSAN RISIKO KESELAMATAN 25
KAWALAN KESELAMATAN ORGANISASI 26
5.1 POLISI KESELAMATAN SIBER 27
5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT 29
5.3 PENGASINGAN TUGAS 37
5.4 PENGURUSAN DAN KAWALAN KESELAMATAN 38
5.5 HUBUNGAN DENGAN PIHAK BERKUASA 39
5.6 HUBUNGAN DENGAN PIHAK BERKEPENTINGAN YANG KHUSUS 40
5.7 KECERDASAN ANCAMAN (THREAT INTELLIGENCE) 41
5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK 41
5.9 INVENTORI MAKLUMAT DAN ASET LAIN YANG BERKAITAN 42
5.10 PENERIMAAN DAN PENGGUNAAN MAKLUMAT DAN ASET ICT 43
5.11 PEMULANGAN ASET 44
5.12 KLASIFIKASI MAKLUMAT 45

5.13PELABELAN MAKLUMAT 46
5.14PEMINDAHAN MAKLUMAT 46
5.15KAWALAN AKSES 47
5.16 PENGURUSAN IDENTITI 49
5.17PENGESAHAN IDENTITI 50
5.18HAK AKSES 52
5.19KESELAMATAN MAKLUMAT DALAM PENGURUSAN PEMBEKAL 52
5.20MENANGANI KESELAMATAN MAKLUMAT DI DALAM PERJANJIAN PEMBEKAL ... 54
5.21MENGURUSKAN KESELAMATAN MAKLUMAT DALAM RANTAIAN BEKALAN ICT .. 55
5.22MEMANTAU, MENGKAJI DAN PENGURUSAN PERUBAHAN PERKHIDMATAN PEMBEKAL 56
5.23KESELAMATAN MAKLUMAT UNTUK PENGGUNAAN PERKHIDMATAN AWAN 57
5.24PELAN DAN PENYEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT 58
5.25PENILAIAN DN KEPUTUSAN INSIDEN KESELAMATAN MAKLUMAT 60
5.26TINDAKBALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT 61
5.27PENGAJARAN DARI INSIDEN KESELAMATAN MAKLUMAT 62
5.28PENGUMPULAN BUKTI 63
5.29KESELAMATAN MAKLUMAT SEMASA GANGGUAN 63
5.30KESEDIAAN ICT UNTUK KESINAMBUNGAN PERKHIDMATAN 64
5.31KEPERLUAN UNDANG-UNDANG, KANUN, PERATURAN DAN KONTRAK 65
5.32HAK HARTA INTELEK 66
5.33PERLINDUNGAN REKOD 66
5.34PRIVASI DAN PELINDUNGAN MAKLUMAT PENGENALAN PERIBADI (PII) 67
5.35KAJIAN BEBAS KESELAMATAN MAKLUMAT 67
5.36PEMATUHAN DENGAN POLISI, PERATURAN DAN PIAWAIAN UNTUK KESELAMATAN MAKLUMAT 68
5.37PROSEDUR OPERASI YANG DIDOKUMENKAN 69
5.38PENGGUNAAN TEKNOLOGI KECERDASAN BUATAN (AI) 70
KAWALAN KESELAMATAN MANUSIA 72
6.1 SARINGAN 73
6.2 TERMA DAN SYARAT PERKHIDMATAN 73
6.3 KESEDARAN, PENDIDIKAN DAN LATIHAN KESELAMATAN MAKLUMAT 74
6.4 PROSES TATATERTIB 75
6.5 PENAMATAN ATAU PERTUKARAN JAWATAN 76

6.6 PERJANJIAN KERAHSIAAN ATAU KETERDEDAHAN 76
6.7 TELEKERJA (REMOTE WORKING) 77
6.8 PELAPORAN INSIDEN KESELAMATAN MAKLUMAT 77
KAWALAN KESELAMATAN FIZIKAL 79
7.2 KEMASUKAN FIZIKAL 81
7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN (FASILITI) 82
7.4 PEMANTAUAN KESELAMATAN FIZIKAL 82
7.5 PERLINDUNGAN DARIPADA ANCAMAN LUAR DAN PERSEKITARAN 84
7.6 BEKERJA DIKAWASAN SELAMAT 85
7.7 MEJA BERSIH DAN SKRIN KOSONG (CLEAR DESK AND CLEAR SCREEN) 86
7.8 PERLINDUNGAN PERALATAN 87
7.9 KESELAMATAN ASET LUAR PREMIS 89
7.10 MEDIA STORAN 89
7.11 UTILITI SOKONGAN 91
7.12 KESELAMATAN KABEL 91
7.13 PENYELENGGARAAN PERALATAN 92
7.14 PELUPUSAN SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN 93
KAWALAN KESELAMATAN TEKNOLOGI 96
8.1 PERANTI PENGGUNA (USER ENDPOINT DEVICES) 97
8.2 HAK AKSES ISTIMEWA 98
8.3 SEKATAN AKSES MAKLUMAT 98
8.4 AKSES KEPADA KOD SUMBER 99
8.5 PENGESAHAN SELAMAT 100
8.6 PENGURUSAN KAPASITI 101
8.7 KAWALAN DARIPADA PERISIAN HASAD (MALWARE) 102
8.8 PENGURUSAN KERENTANAN TEKNIKAL 103
8.9 PENGURUSAN KONFIGURASI 104
8.10 PEMADAMAN MAKLUMAT 105
8.11 PENYEMBUNYIAN DATA (*DATA MASKING*) 105
8.12 PENCEGAHAN KEBOCORAN DATA (*DATA LEAK PREVENTION*) 106
8.13 SANDARAN MAKLUMAT (BACKUP) 107
8.14 PERTINDIHAN KEMUDAHAN PEMPROSESAN MAKLUMAT 108
8.15 PENGELOGAN 110

8.16PEMANTAUAN AKTIVITI ICT 111
8.17PENYERAGAMAN JAM 112
8.18PENGGUNAAN PROGRAM UTILITI 112
8.19PEMASANGAN PERISIAN PADA SISTEM OPERASI 113
8.20KESELAMATAN RANGKAIAN 114
8.21KESELAMATAN PERKHIDMATAN 115
8.22PENGASINGAN RANGKAIAN 115
8.23PENAPISAN LAMAN (WEB) 116
8.24PENGGUNAAN KRIPTOGRAFI 117
8.25KITARAN HAYAT PEMBANGUNAN SISTEM/APLIKASI YANG SELAMAT 118
8.26KEPERLUAN KESELAMATAN APLIKASI 119
8.27SENIBINA SISTEM SELAMAT DAN PRINSIP KEJURUTERAAN 120
8.28PENGEKODAN SELAMAT 121
8.29UJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN 122
8.30PEMBANGUNAN OLEH SUMBER LUAR (*OUTSOURCE*) 123
8.31PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PENGELUARAN (PRODUCTION) 124
8.32PENGURUSAN PERUBAHAN 125
8.33MAKLUMAT UJIAN 126
8.34PERLINDUNGAN SISTEM MAKLUMAT ICT SEMASA PENGUJIAN/PENGAUDITAN 127
JADUAL MAPPING ANNEX 27001:2022 KEPADA BIDANG PKS KPT VERSI 2 128
SENARAI PERUNDANGAN DAN PERATURAN YANG BERKAITAN 134
REKOD PINDAAN DOKUMEN 137
LAMPIRAN 1 139
LAMPIRAN 2 140

PENGENALAN



1.0 PENGENALAN

Polisi Keselamatan Siber (PKS) KPT mengandungi peraturan yang MESTI DIBACA dan DIPATUHI semasa menggunakan aset dan menjalankan operasi penyampaian perkhidmatan KPT. Polisi ini juga menerangkan kepada warga KPT dan pihak luar yang terlibat dengan perkhidmatan KPT tentang tanggungjawab dan peranan mereka dalam melindungi maklumat dan aset KPT.

Maklumat merupakan aset utama (sama ada dalam bentuk fizikal atau elektronik) yang bernilai tinggi kepada KPT. Keselamatan maklumat dilaksanakan untuk melindungi kerahsiaan, integriti dan ketersediaan maklumat dan aset perkhidmatan KPT. Langkah ini juga bertujuan untuk melindungi maklumat daripada risiko (ancaman dan kelemahan) yang boleh mengganggu kesinambungan perkhidmatan. Keselamatan maklumat dilaksanakan melalui perancangan, pembangunan, pengujian dan penyelenggaraan bagi mengekalkan keberkesanannya dalam menyokong pencapaian objektif perkhidmatan, mengekalkan imej dan meningkatkan pematuhan kepada undang-undang.

Pada era ini, keselamatan maklumat sangat bergantung pada aset Teknologi Maklumat dan Komunikasi (ICT). Oleh itu, polisi ini juga menitikberatkan keselamatan infrastruktur dan infostruktur KPT bagi memastikan perkhidmatan yang diberikan tepat dan selamat.

PKS KPT ini dibangunkan selaras dengan amalan terbaik dan keperluan standard antarabangsa ISO/IEC 27001:2022 *Information Security Management System* (ISMS). PKS ini juga tertakluk pada dan mematuhi ketetapan undang-undang di bawah Akta Keselamatan Siber 2024 [Akta 854] serta Tataamalan bagi Entiti Infrastruktur Maklumat Kritikal Negara (NCII) Sektor Kerajaan yang ditetapkan oleh Jabatan Digital Negara (JDN). Penjajaran ini bertujuan untuk memastikan setiap langkah, standard, dan proses kawalan keselamatan siber KPT dilaksanakan secara berstruktur, meminimumkan risiko ancaman secara berkesan, dan memastikan tahap perlindungan NCII sentiasa berada pada tahap yang optimum.

1.1 OBJEKTIF

Dokumen PKS KPT ini dibangunkan untuk mencapai objektif berikut:

a. Menerangkan kepada semua pengguna yang merangkumi warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT;
b. Memastikan keselamatan penyampaian perkhidmatan KPT berada pada tahap tertinggi, sekali gus meningkatkan keyakinan pihak berkepentingan seperti agensi kerajaan, industri dan orang awam;
c. Memastikan kelancaran operasi KPT dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;

d. Melindungi kepentingan pihak-pihak yang bergantung pada sistem maklumat daripada kesan kegagalan atau kelemahan yang berlaku dari segi kerahsiaan, integriti, ketersediaan, kesahihan maklumat dan komunikasi; dan
e. Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

1.2 SKOP

Dokumen PKS KPT ini adalah selaras dengan Standard ISO/IEC 27001:2022 Keselamatan Maklumat, Keselamatan Siber dan Perlindungan Privasi – Kawalan Keselamatan Maklumat yang meliputi bidang keselamatan berikut:

a. Pengurusan Risiko Keselamatan Maklumat;
b. Kawalan Keselamatan Organisasi;
c. Kawalan Keselamatan Manusia;
d. Kawalan Keselamatan Fizikal; dan
e. Kawalan Keselamatan Teknologi.

1.3 PERANAN DAN TANGGUNGJAWAB

Ketua Setiausaha KPT hendaklah bertanggungjawab sepenuhnya dalam melaksanakan semua bidang kawalan yang digariskan dalam PKS KPT dan memastikan polisi ini dipatuhi oleh semua warga KPT dan pihak ketiga yang berurusan dengan perkhidmatan KPT.

Peranan dan tanggungjawab setiap pihak yang terlibat dalam mencapai objektif PKS KPT diterangkan dengan lebih jelas dalam Kawalan 5.2 Peranan dan Tanggungjawab Keselamatan Maklumat.

1.4 PEMAKAIAN

Polisi ini terpakai kepada semua Warga KPT, pembekal dan pihak ketiga yang berurusan dengan perkhidmatan KPT.

1.5 PENGUATKUASAAN DAN SEMAKAN

Polisi ini berkuat kuasa mulai tarikh diluluskan dan disemak setiap tahun atau jika terdapat arahan terkini atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan dan polisi kerajaan bagi memastikan dokumen sentiasa relevan.

Pelanggaran PKS KPT ini boleh mengakibatkan tindakan tatatertib, amaran atau teguran. Perbuatan seperti tidak tahu, tidak berniat baik atau menggunakan pertimbangan yang buruk tidak boleh digunakan sebagai alasan untuk ketidakpatuhan.

1.6 PERINGATAN PENTING

a. Semua pengguna bertanggungjawab :
   i. Memastikan klasifikasi maklumat itu diwujudkan mengikut empat (4) klasifikasi maklumat iaitu Rahsia, Sulit, Terhad dan Terbuka;
   ii. Mengendalikan maklumat tersebut mengikut tahap klasifikasi/ pengelasannya;
   iii. Mematuhi polisi, prosedur, dan sebarang keperluan kontrak/ perjanjian KPT; dan
   iv. Melindungi maklumat MPP yang terdiri daripada data peribadi dan data sensitif individu.

b. Maklumat mesti dilindungi daripada akses dan pemprosesan yang tidak dibenarkan.

c. Kawalan keselamatan maklumat dan polisi/ konfigurasi yang dipasang hendaklah disemak secara berkala, termasuk audit dalaman/ luaran tahunan dan ujian penembusan. Di samping itu, kawalan keselamatan maklumat hendaklah ditetapkan berdasarkan penilaian risiko yang mengambil kira perubahan ancaman dan kelemahan pada aset maklumat tersebut.

1.7 RUJUKAN

BIL	NAMA DOKUMEN	NOMBOR	TERBITAN
a.	*Information Technology Security – Information Security Management System Requirements (3rd Revision)*	ISO/IEC 27001:2022	*International Standard*
b.	*Information Technology Security Techniques-Code of Practices for Information Security Controls (3rd Revision)*	ISO/IEC 27002:2022	*International Standard*
c.	Buku Arahan Keselamatan (semakan dan Pindaan 2017)	-	2017
d.	Akta Keselamatan Siber 2024 (Akta 854)	-	2024
e.	Tataamalan JDN v.1.3	-	2025

1.8 PERTANYAAN

Sebarang pertanyaan mengenai PKS KPT ini boleh dikemukakan kepada:

Unit Keselamatan ICT

Bahagian Pengurusan Maklumat,

Kementerian Pendidikan Tinggi

E-mel : cybersec@mohe.gov.my

GLOSARI / TERMA RUJUKAN



2.0 GLOSARI / TERMA RUJUKAN

2.1 GLOSARI

BCP	*Business Continuity Plan* (Pelan Kesinambungan Perkhidmatan)
BYOD	*Bring Your Own Device* (Peranti Peribadi)
CCTV	*Closed-Circuit Television* (Televisyen Litar Tertutup)
CDO	Ketua Pegawai Digital / *Chief Digital Officer*
DLP	*Data Leakage Prevention* (Pencegahan Ketirisan Data)
GCERT	*Government Computer Emergency Response Team*
HTTPS	*Hyper Text Transfer Protocol Secure*
ICERT	*Computer Emergency Response Team*
ICT	*Information and Communication Technology*
ICTSO	*ICT Security Officer* (Pegawai Keselamatan Maklumat)
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
JDN	Jabatan Digital Negara
JPICT	Jawatankuasa Pemandu ICT
PKS	Polisi Keselamatan Siber
KSU	Ketua Setiausaha
LAN	*Local Area Network*
MFA	*Multi-Factor Authentication* (Pengesahan Berbilang Faktor)
NACSA	*National Cyber Security Agency* (Agensi Keselamatan Siber Negara)
NCII	*National Critical Information Infrastructure* (Infrastruktur Maklumat Kritikal Negara)
NDA	*Non-Disclosure Agreement* (Perjanjian Kerahsiaan)

PII	Maklumat Pengenalan Peribadi (*Personally Identifiable Information*)
PKI	*Public-Key Infrastructure*
SSL	*Secure Sockets Layer*
UPS	*Uninterruptible Power Supply*
UKTN	Unit Keselamatan Teknikal Naziran
WAN	*Wide Area Network*

2.2 TERMA RUJUKAN

Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM untuk sebarang kemungkinan adanya virus.
Aset Alih	Aset alih merujuk kepada aset yang boleh dipindahkan dari satu tempat ke tempat lain, termasuk aset yang dibekalkan atau dipasang bersama bangunan.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup (Sandaran)	Proses penduaan sesuatu dokumen atau maklumat.
Baki risiko	Risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan.
Bandwidth	Jalur lebar. Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
Clear Desk dan *Clear Screen*	Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
Data-at-rest (data-dalam simpanan)	Merujuk kepada data yang disimpan dalam sistem destinasi yang stabil. *Data at rest* lazimnya ditakrifkan sebagai data

	yang tidak sedang digunakan atau tidak sedang dihantar ke titik akhir sistem, seperti peranti mudah alih atau stesen kerja.
Data-in-motion (data-dalam pergerakan)	Merujuk kepada aliran data yang bergerak melalui sebarang jenis rangkaian. Ia menggambarkan data yang sedang dipindahkan atau dihantar.
Data-in-use (data-dalam penggunaan)	Merujuk kepada data yang tidak sekadar disimpan secara pasif dalam destinasi yang stabil, seperti gudang data berpusat, tetapi sedang diproses atau bergerak melalui komponen lain dalam seni bina teknologi maklumat.
Denial of service	Halangan pemberian perkhidmatan
Defense-in-depth	Pendekatan keselamatan siber yang menggunakan mekanisme pertahanan berlapis untuk melindungi data dan maklumat.
Downloading	Aktiviti muat turun sesuatu perisian.
Encryption	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
Hab (*Hub*)	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain.
Impak teknikal	Melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti.

Impak fungsi jabatan	Melibatkan perkara-perkara dari segi kewangan, reputasi, ketidakpatuhan dan pelanggaran privasi.
Insiden keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian tersebut agar sentiasa berasingan.
Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan.
Kriptografi	Kaedah untuk menukar data dan maklumat biasa (*standard format*) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
Lock	Mengunci komputer.
Logout	Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan *virus, trojan horse, worm*, *spyware* dan sebagainya.
Mobile Code	Merupakan suatu perisian yang boleh dipindahkan di antara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh *Java Applet*, *ActiveX* dan sebagainya pada pelayar internet.

MODEM	*MOdulator DEModulator* ; peranti yang boleh menukar *strim bit digital* ke isyarat analog dan sebaliknya. Kebiasaannya disambung ke talian telefon bagi membolehkan capaian internet dibuat dari komputer.
Outsource	Menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan dokumen perjanjian dengan bayaran yang dipersetujui.
Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
Pengguna	Warga KPT, pembekal dan pihak-pihak lain yang diberi kebenaran menggunakan perkhidmatan ICT KPT.
Pengolahan risiko	Tindakan yang merangkumi elemen proses, teknologi dan manusia, yang hendaklah dikenal pasti dan dilaksanakan berdasarkan hasil penilaian risiko.
Perisian Aplikasi	Merujuk kepada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Rollback (undur)	Pengembalian pangkalan data atau program kepada keadaan stabil sebelum sesuatu ralat berlaku.
Ruang siber	Sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem tersebut secara fizikal atau maya serta persekitaran fizikal sistem tersebut dan semua aset yang berkaitan dengan ICT.
Screen saver	Imej yang akan diaktifkan pada sistem/komputer setelah ia tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer.
Source Code	Kod Sumber atau kod program (biasanya hanya dipanggil sumber atau kod) merujuk kepada sebarang siri pernyataan

	yang ditulis dalam bahasa pengaturcaraan komputer yang difahami manusia.
Switch	*Switch* (Suis) ialah gabungan fungsi hab dan titi (bridge) yang menapis bingkai data bagi membolehkan segmentasi rangkaian. Penggunaan suis dapat meningkatkan prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (*CSMA/CD*), iaitu satu kaedah penghantaran data, dengan mengurangkan berlakunya pelanggaran (*collision*).
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna pada masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.
Worm	Sejenis virus yang boleh bereplikasi dan membiak dengan sendiri, yang biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.

KESELAMATAN

MAKLUMAT DAN PENGURUSAN MAKLUMAT



KESELAMATAN MAKLUMAT DAN PENGURUSAN MAKLUMAT MERANGKUMI TAKRIF, PRINSIP, CIRI-CIRI DAN KATEGORI MAKLUMAT YANG DILINDUNGI

3.0 KESELAMATAN MAKLUMAT DAN PENGURUSAN MAKLUMAT

3.1 TAKRIF KESELAMATAN MAKLUMAT DAN PENGURUSAN MAKLUMAT:

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

b. **Keselamatan Maklumat** ditakrifkan sebagai melindungi semua bentuk maklumat elektronik (ICT) dan bukan elektronik yang dimasukkan, dicipta, dimusnahkan, disimpan, dijana, dicetak, diakses, diedarkan, dalam penghantaran dan disalin bagi memastikan keselamatan dan ketersediaan maklumat kepada semua pengguna yang dibenarkan.

c. **Keselamatan Siber** ditakrifkan sebagai perlindungan terhadap semua peranti ICT (perkakasan dan perisian) serta data dalam ruang siber atau internet.

d. **Keselamatan ICT** ditakrifkan sebagai keadaan apabila segala urusan menyediakan dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan.

3.2 PRINSIP-PRINSIP KESELAMATAN MAKLUMAT

Prinsip keselamatan hendaklah dipilih berdasarkan penilaian risiko dan kategori maklumat yang dikendalikan oleh sistem. Bagi mencapai objektif keselamatan maklumat, KPT hendaklah melaksanakan prinsip keselamatan seperti yang berikut:

a. Prinsip “Perlu-Tahu”

Kementerian Pendidikan Tinggi (KPT) hendaklah melaksanakan mekanisme kawalan akses maklumat berdasarkan prinsip "Perlu-Tahu" (*Need-to-Know*). Pengguna hanya dibenarkan mengakses maklumat yang diperlukan untuk melaksanakan tugas mereka. Bagi capaian spesifik terhadap Maklumat Rahsia Rasmi, kebenaran akses hendaklah dihadkan mengikut parameter masa, lokasi, peranan dan fungsi pengguna.

b. Hak Keistimewaan Minimum

Setiap pengguna hendaklah diberikan hak keistimewaan minimum yang mencukupi bagi melaksanakan tugas mereka. Akses hanya diberikan pada tahap yang paling minimum, seperti hak membaca dan/atau melihat sahaja.

Kelulusan diperlukan bagi membolehkan pengguna mencipta, menyimpan, mengemas kini, mengubah atau membatalkan maklumat. Hak akses ini perlu dikaji secara berkala berdasarkan peranan dan tanggungjawab pengguna.

c. Akauntabiliti

Setiap pengguna bertanggungjawab terhadap semua aset ICT, hak capaian dan tindakan yang dilakukan menggunakan akaun mereka. Segala aktiviti pengguna hendaklah direkodkan dan diawasi bagi memastikan kepatuhan terhadap polisi keselamatan maklumat.

d. Pengasingan Tugas

Bagi mengekalkan prinsip sekat-dan-imbang (*check and balance*), KPT hendaklah melaksanakan pengasingan tugas bagi tugas-tugas kritikal. Ini bertujuan untuk mengelakkan pelaksanaan tugas kritikal oleh seorang pengguna secara tunggal tanpa sebarang mekanisme pemantauan atau semakan oleh pihak lain.

e. Pengauditan

KPT hendaklah melaksanakan aktiviti pengauditan secara berkala bagi mengenal pasti sebarang ketidakakuran keselamatan atau ancaman yang boleh menjejaskan keselamatan sistem. Semua rekod berkaitan tindakan keselamatan hendaklah dipelihara dan disimpan. Aset ICT seperti komputer, pelayan (*server*), penghala (*router*), tembok api (*firewall*), Sistem Pencegahan Pencerobohan (IPS), perisian *antivirus* dan peralatan rangkaian lain hendaklah mampu menjana dan menyimpan log keselamatan serta jejak audit (*audit trail*).

f. Pemulihan

Proses pemulihan sistem adalah penting untuk memastikan kesinambungan perkhidmatan dan kebolehcapaian data. Objektif utama adalah untuk meminimumkan gangguan atau kerugian akibat insiden keselamatan atau bencana. Pemulihan boleh dilakukan melalui aktiviti sandaran (*backup*) yang berkala serta pelaksanaan Pelan Pemulihan Bencana (*Disaster Recovery Plan*, DRP) dan Pelan Kesinambungan Perkhidmatan (*Business Continuity Plan*, BCP).

g. Saling bergantungan

Setiap prinsip yang digariskan adalah saling melengkapi dan bergantungan antara satu sama lain. Oleh itu, pendekatan yang pelbagai perlu diterapkan dalam penyusunan mekanisme keselamatan untuk mencapai tahap perlindungan maksimum. KPT tidak boleh hanya bergantung pada individu, organisasi, atau peralatan tertentu dalam melaksanakan keselamatan ICT. Sebaliknya, pelbagai kawalan keselamatan perlu diterapkan bagi memastikan perlindungan menyeluruh terhadap aset maklumat.

3.3 CIRI-CIRI KESELAMATAN MAKLUMAT

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 terkini dan hanya boleh diubah dengan cara yang dibenarkan.

c. Tidak Boleh Disangkal

Data dan maklumat hendaklah berasal daripada sumber yang sah dan tidak boleh disangkal.

d. Kesahihan

Data dan maklumat hendaklah dipastikan kesahihannya.

e. Ketersediaan

Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

3.4 KATEGORI MAKLUMAT

a. Maklumat Rahsia Rasmi

Di bawah Akta Rahsia Rasmi 1972 (Akta 88), maksud Maklumat Rahsia Rasmi ialah apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 (Akta 88) dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad” mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972.

b. Maklumat Rasmi

Maklumat rasmi ialah maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh KPT semasa menjalankan urusan rasmi. Maklumat rasmi ini juga merupakan rekod awam yang tertakluk pada peraturan-peraturan Arkib Negara.

c. Maklumat Pengenalan Peribadi (*Personally Identifiable Information* (PII))

Maklumat Pengenalan Peribadi (*Personally Identifiable Information* (PII)) ialah maklumat yang boleh digunakan secara tersendiri atau digunakan bersama

maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu. PII boleh juga terkandung dalam Maklumat Rahsia Rasmi.

d. Data Terbuka

Data terbuka merujuk kepada data kerajaan yang boleh digunakan secara bebas, boleh dikongsi dan digunakan semula oleh rakyat, agensi sektor awam atau swasta untuk sebarang tujuan. PII dikecualikan daripada data terbuka.

e. Maklumat/ Data Bukan Elektronik

Maklumat dalam bentuk dokumen fizikal seperti surat, memo, dokumentasi, prosedur operasi, rekod-rekod, maklumat arkib dan lain-lain.

4.0 PENGURUSAN RISIKO KESELAMATAN

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

KPT hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala iaitu sekurang-kurangnya sekali setahun dan berterusan bergantung pada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya, KPT hendaklah mengambil tindakan susulan dan/ atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

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

Bagi aset ICT yang dikategorikan sebagai Infrastruktur Maklumat Kritikal Negara (NCII), laporan penilaian risiko keselamatan ICT hendaklah dikemukakan kepada Agensi Keselamatan Siber Negara (NACSA) dan Jabatan Digital Negara (JDN) dalam tempoh 30 hari selepas penilaian selesai dilaksanakan.

KPT bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 3 Tahun 2024: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam Bertarikh 21 Mac 2024.

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

a. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
b. Menerima dan/atau bersedia menghadapi risiko yang mungkin berlaku selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi.
c. Mengelakkan dan/atau mencegah berlakunya risiko melalui tindakan yang bersesuaian; dan
d. Memindahkan risiko kepada pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

KAWALAN

KESELAMATAN ORGANISASI

KAWALAN KESELAMATAN ORGANISASI MERANGKUMI PERATURAN DAN LANGKAH YANG MENENTUKAN SIKAP KOMPREHENSIF ORGANISAS TERHADAP PERLINDUNGAN DATA DALAM PELBAGA PERKARA. KAWALAN INI TERMASUK POLISI, PERATU PROSES, PROSEDUR ORGANISASI DAN SEBAGAINYA



5.1 POLISI KESELAMATAN SIBER



OBJEKTIF:
Memastikan kesesuaian, kecukupan dan keberkesanan berterusan hala tuju pengurusan dan sokongan untuk keselamatan maklumat selaras dengan keperluan perkhidmatan, undang-undang, berkanun, peraturan dan kontrak.

POLISI	PERANAN
5.1.1 Pelaksanaan Polisi	
a. Pelaksanaan polisi akan dijalankan oleh Ketua Setiausaha (KSU) KPT dengan disokong oleh Jawatankuasa Pemandu ICT (JPICT) yang terdiri daripada Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO) dan ahli-ahli yang dilantik oleh KSU KPT.	KSU CDO ICTSO SUB (BPM)
5.1.2 Penyebaran Polisi	
a. Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan KPT kepada warga KPT, pembekal serta pihak berkepentingan yang mempunyai urusan dengan perkhidmatan ICT KPT.	ICTSO
5.1.3 Penyelenggaraan Polisi	
a. Polisi ini perlu disemak dan dikaji semula sekurang-kurangnya setahun sekali atau mengikut keperluan semasa bagi memastikan dokumen ini sentiasa relevan; b. PKS KPT adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar kerajaan dan kepentingan sosial;	ICTSO

c. Semakan tahunan, pindaan dan pembetulan *minor/subversi* hanya perlu dibentangkan dalam Jawatankuasa ISMS (JK ISMS), manakala pindaan dan pembetulan *major* perlu dibentangkan dan mendapat kelulusan Jawatankuasa–Pemandu ICT (JPICT) KPT; dan d. Memaklumkan pindaan yang telah disahkan kepada Warga KPT, pembekal dan pihak berkepentingan yang mempunyai urusan dengan perkhidmatan ICT KPT.	
5.1.4 Penguatkuasaan Polisi	
a. Polisi Keselamatan Siber (PKS) KPT terpakai kepada semua Warga KPT, pembekal dan pihak berkepentingan yang menggunakan perkhidmatan Siber KPT. b. Sebarang pelanggaran atau ketidakpatuhan terhadap polisi ini sama ada disengajakan atau tidak disengajakan boleh mengakibatkan tindakan pembetulan, pelaksanaan kawalan keselamatan tambahan atau tindakan tatatertib mengikut peraturan dan perundangan yang berkuat kuasa. c. Ketidakpatuhan terhadap keperluan keselamatan siber juga boleh mengakibatkan pengeluaran arahan pembetulan yang dikeluarkan oleh Ketua Eksekutif Agensi Keselamatan Siber Negara (NACSA) serta tertakluk kepada obligasi dan peruntukan undang-undang di bawah Akta Keselamatan Siber 2024 [Akta 854]	Warga KPT Pihak ketiga

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT



OBJEKTIF:
Mewujudkan struktur yang ditakrifkan, diluluskan dan difahami untuk pelaksanaan, operasi dan pengurusan keselamatan maklumat dalam organisasi.

POLISI	PERANAN
5.2.1 Ketua Setiausaha (KSU)	
Memastikan penguatkuasaan pelaksanaan Polisi ini; a. Memastikan Warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT memahami dan mematuhi peruntukan-peruntukan di bawah polisi ini; b. Memastikan semua keperluan KPT seperti sumber kewangan, personel dan perlindungan keselamatan adalah mencukupi; c. Memastikan pengurusan risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan dalam polisi ini; dan d. Melantik CDO dan ICTSO.	KSU
5.2.2 Ketua Pegawai Digital (CDO)	
a. Membantu Ketua Setiausaha melaksanakan tanggungjawab keselamatan ICT seperti yang ditetapkan dalam polisi ini; b. Memastikan kawalan keselamatan maklumat dan tadbir urus inisiatif digital KPT diseragamkan, diselaraskan dan dilaksanakan dengan berkesan serta mematuhi peraturan keselamatan siber yang berkuat kuasa; c. Memastikan aspek keselamatan ICT diterapkan dalam Pelan Strategik Pendigitalan KPT;	CDO

d. Menyelaras pelan latihan dan program kesedaran keselamatan ICT; e. Menilai dan mengintegrasikan keperluan keselamatan siber dalam penggunaan teknologi digital baharu bagi memastikan pelaksanaan yang selamat tanpa menjejaskan inovasi; dan f. Memastikan kesediaan pengurusan keselamatan siber serta perlindungan data dan privasi dalam semua inisiatif digital KPT selaras dengan peraturan yang berkaitan.	
5.2.3 Pegawai Keselamatan ICT (ICTSO)	
a. Membangunkan serta menyebarkan polisi dan langkah-langkah keselamatan ICT kepada Warga KPT; b. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS ini; c. Merangka pengurusan risiko dan audit keselamatan siber berpandukan rangka kerja, polisi dan pekeliling/garis panduan yang berkuat kuasa; d. Menyediakan dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlakunya ancaman keselamatan siber dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; e. Melaporkan insiden keselamatan siber kepada CSIRT KPT dan seterusnya membantu dalam penyiasatan atau pemulihan; f. Melaporkan insiden keselamatan siber kepada CDO bagi insiden yang memerlukan Pengurusan Kesinambungan Perkhidmatan (PKP); g. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden	ICTSO

keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera; h. Memastikan pematuhan terhadap polisi ini oleh Warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan Siber KPT; i. Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber; j. Menyediakan dan merangka latihan dan program kesedaran keselamatan siber; dan k. Melantik tiga (3) orang individu yang diberi kuasa khusus untuk membuat pemberitahuan insiden keselamatan siber seperti yang dikehendaki dalam Arahan Ketua Eksekutif NACSA No. 1. l. Mempromosikan bidang kawalan yang digariskan dalam tataamalan JDN m. Memastikan tataamalan JDN dipatuhi sepenuhnya oleh semua pihak yang terlibat dalam mengendalikan infrastruktur maklumat kritikal negara.	
5.2.4 Jawatankuasa Pemandu ICT (JPICT)	
Keanggotaan JPICT KPT adalah seperti berikut : Pengerusi : Ketua Setiausaha KPT Ahli : Pegawai-pegawai di KPT yang telah dilantik. Pegawai-pegawai di UA yang telah dilantik Tanggungjawab yang perlu dilaksanakan seperti berikut: a. Peranan dan tanggungjawab JPICT KPT adalah seperti yang terkandung dalam Surat Pekeliling Am Bil. 3 Tahun 2015 iaitu merancang dan menentukan langkah-langkah keselamatan siber.	JPICT

5.2.4 Jawatankuasa ISMS	
Keanggotaan JK ISMS KPT adalah seperti berikut : Pengerusi : Setiausaha BPM Ahli : Pegawai-pegawai di KPT yang telah dilantik. Tanggungjawab yang perlu dilaksanakan seperti berikut: a. Bertanggungjawab menyelaras pelaksanaan keselamatan maklumat, membuat keputusan berkaitan risiko, memastikan pematuhan kepada dasar dan standard, serta memupuk budaya keselamatan dalam organisasi; dan b. Mengkaji, menyemak dan meluluskan sebarang pindaan minor Polisi Keselamatan Siber (PKS), garis panduan dan Prosedur Operasi Standard (SOP) Keselamatan Siber.	JK ISMS
5.2.5 Setiausaha Bahagian (Bahagian Pengurusan Maklumat)	
Tanggungjawab yang perlu dilaksanakan seperti berikut: a. Menyelaras pembangunan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu; dan b. Mengurus perolehan, naik taraf atau peningkatan perisian serta sistem komputer bagi memastikan kesesuaian, keselamatan dan keupayaan operasi sentiasa terpelihara; dan c. Menyelaras perolehan teknologi dan perkhidmatan komunikasi baharu, merangkumi penilaian keperluan, kesediaan infrastruktur dan pematuhan kepada dasar berkaitan; dan d. Memastikan pembekal dan rakan usaha sama menjalani tapisan keselamatan; dan e. Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi dan pekeliling/garis panduan berkuat kuasa.	SUB (BPM)

5.2.6 CSIRT KPT	
Keanggotaan CSIRT KPT adalah seperti berikut : Pengarah CSIRT : SUB BPM Pengurus CSIRT : KPSU(M)TT Ahli CSIRT :Pegawai-pegawai Teknologi Maklumat di Bahagian Pengurusan Maklumat KPT yang telah dilantik. Tanggungjawab yang perlu dilaksanakan seperti berikut: a. Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden; b. Merekodkan dan menjalankan siasatan awal insiden yang diterima; c. Menangani tindak balas insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d. Menasihati Pentadbir Sistem/Pentadbir Pusat Data untuk mengambil tindakan pemulihan dan pengukuhan; e. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada Pentadbir Sistem ICT; dan f. Melaksanakan prinsip-prinsip PKS KPT dalam melindungi kerahsiaan maklumat KPT.	CSIRT
5.2.7 Pentadbir Rangkaian	
Pentadbir Rangkaian ICT berperanan menguruskan rangkaian di KPT. Pentadbir Rangkaian ICT hendaklah melaksanakan tanggungjawab seperti berikut: a. Menyelaras, memantau, menyelenggara, mengkonfigurasi dan memberikan sokongan teknikal bagi infrastruktur rangkaian LAN dan WIFI KPT;	Pentadbir Rangkaian

b. Menyelaras, memantau, menyelenggara dan memberi sokongan teknikal bagi sistem keselamatan rangkaian; dan c. Melaksanakan prinsip-prinsip PKS KPT dan melindungi kerahsiaan maklumat KPT.	
5.2.8 Pentadbir Pusat Data	
Pentadbir Pusat Data berperanan menguruskan keseluruhan Pusat Data KPT. Pentadbir Pusat Data hendaklah melaksanakan tanggungjawab seperti berikut: a. Menyelaras, memantau, menyelenggara, mengkonfigurasi dan memberi sokongan teknikal untuk semua aktiviti dan infrastruktur yang melibatkan pengurusan pusat data dan DRC KPT; b. Melaksanakan dan mengemas kini penilaian dan pengolahan risiko; c. Melaksanakan kawalan keselamatan yang bersesuaian; dan d. Melaksanakan prinsip-prinsip PKS KPT dan melindungi kerahsiaan maklumat KPT.	Pentadbir Pusat Data
5.2.9 Pentadbir E-mel	
Pentadbir e-mel berperanan mentadbir semua e-mel di KPT. Pentadbir e-mel hendaklah melaksanakan tanggungjawab seperti berikut: a. Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar dasar atau tatacara jabatan) perlulah dilakukan dengan segera atas persetujuan keselamatan maklumat; dan	Pentadbir E-mel

b. Melaksanakan pembekuan akaun sekiranya diperlukan, terutamanya semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib.	
5.2.10 Pentadbir Sistem	
Pentadbir Sistem hendaklah melaksanakan tanggungjawab seperti berikut: a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai personel yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesahihan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan dalam polisi ini; c. Memantau aktiviti capaian sistem aplikasi; d. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta; e. Menganalisis dan menyimpan rekod jejak audit; dan f. Menyediakan laporan mengenai aktiviti capaian secara berkala.	Pentadbir Sistem
5.2.11 Pemilik Sistem	
Sesuatu sistem hendaklah dimiliki oleh sesuatu Unit atau Bahagian di KPT yang mempunyai kepentingan terhadap sistem tersebut. Pemilik Sistem terdiri daripada Ketua Jabatan/Unit/Bahagian yang merupakan pemilik bisnes/proses bagi sistem yang dibangunkan. Pemilik sistem bertanggungjawab melaksanakan perkara berikut:	Pemilik Sistem

a. Menentukan klasifikasi maklumat dalam sistem tersebut; b. Melaksanakan kawalan keselamatan yang bersesuaian; c. Menentukan tempoh masa maklumat yang disimpan; dan d. Melaksanakan prinsip-prinsip PKS KPT serta melindungi kerahsiaan maklumat KPT.	
5.2.12 Warga KPT	
a. Membaca, memahami dan mematuhi Polisi ini; b. Mengetahui dan memahami implikasi tindakannya terhadap keselamatan ICT; c. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; d. Mematuhi prinsip-prinsip keselamatan Polisi ini dan menjaga kerahsiaan maklumat Kerajaan; e. Melaksanakan langkah-langkah perlindungan seperti yang berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan maklumat; v. Mematuhi polisi, piawaian dan garis panduan keselamatan ICT yang ditetapkan; vi. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan kawalan keselamatan ICT dari diketahui umum.	Warga KPT

f. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada CSIRT KPT dengan segera; g. Menghadiri program-program kesedaran mengenai keselamatan ICT; h. Bersetuju dengan terma dan syarat yang terkandung di dalam Polisi ini; dan **i.** Menandatangani **Surat Akuan Pematuhan PKS KPT.**	
5.2.13 Pihak Ketiga	
Pihak ketiga terdiri daripada pembekal, pakar perunding, kontraktor, pengguna agensi kerajaan atau swasta dan pihak yang berurusan dengan KPT. Tanggungjawab yang perlu dilaksanakan adalah seperti berikut: a. Membaca, memahami dan mematuhi PKS KPT; b. Bersetuju dengan terma dan syarat yang terkandung di dalam Polisi ini; dan c. Menandatangani **Surat Akuan Pematuhan PKS KPT (LAMPIRAN 2)** dan **Akta Rahsia Rasmi 1972 (Akta 88) Lampiran E dan Lampiran F;**	Pihak Ketiga

5.3 PENGASINGAN TUGAS

OBJEKTIF :
Mengurangkan risiko pengubahsuaian tanpa kebenaran, perubahan yang tidak disengajakan atau penyalahgunaan aset ICT.

POLISI	PERANAN
Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan risiko pengubahsuaian tanpa kebenaran, perubahan yang tidak disengajakan atau penyalahgunaan aset ICT.	SUB Bahagian Warga KPT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b. Tugas mewujudkan, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; c. Perkakasan yang digunakan bagi tugas membangunkan, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan d. Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.	

5.4 PENGURUSAN DAN KAWALAN KESELAMATAN



OBJEKTIF :
Memastikan pengurusan memahami peranan dan tanggungjawab masing-masing dalam keselamatan maklumat dan privasi serta melaksanakan tindakan yang sebaiknya.

POLISI	PERANAN
Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan pengguna ICT diberi taklimat mengenai peranan dan tanggungjawab keselamatan maklumat mereka sebelum diberikan	KSU CDO

capaian kepada maklumat sulit atau sistem maklumat; b. Memastikan pengguna ICT disediakan dengan garis panduan untuk menyatakan jangkaan keselamatan maklumat mengenai peranan mereka dalam KPT; c. Memastikan pengguna ICT mencapai tahap kesedaran mengenai keselamatan maklumat yang berkaitan dengan peranan dan tanggungjawab mereka dalam KPT; d. Memastikan pengguna ICT mematuhi terma dan syarat perkhidmatan, termasuk dasar keselamatan maklumat organisasi dan kaedah kerja yang sesuai; dan e. Memastikan pengguna ICT disediakan saluran pelaporan untuk melaporkan pelanggaran polisi atau prosedur.	

5.5 HUBUNGAN DENGAN PIHAK BERKUASA



OBJEKTIF :
Memastikan aliran maklumat yang sesuai berlaku berkenaan dengan keselamatan maklumat antara organisasi dan pihak berkuasa undang-undang, kawal selia dan penyeliaan yang berkaitan.

POLISI	PERANAN
Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab KPT;	Pasukan CSIRT

b. Mewujudkan dan mengemas kini prosedur/senarai pihak berkuasa perundangan/pihak yang perlu dihubungi semasa kecemasan; c. Pihak berkuasa yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba; dan d. Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.	

5.6 HUBUNGAN DENGAN PIHAK BERKEPENTINGAN YANG KHUSUS



OBJEKTIF:
Memastikan aliran maklumat yang sesuai berlaku berkenaan dengan keselamatan maklumat.

POLISI	PERANAN
Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional ataupun forum bagi: a. Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat; b. Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini; c. Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan d. Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	Pasukan CSIRT

5.7 KECERDASAN ANCAMAN (THREAT INTELLIGENCE)



OBJEKTIF:
Memberi kesedaran tentang ancaman keselamatan siber terhadap organisasi supaya tindakan mitigasi yang sewajarnya dapat diambil.

POLISI	PERANAN
Maklumat tentang ancaman sedia ada atau yang berkemungkinan berlaku hendaklah dikumpulkan dan dianalisis bagi membolehkan tindakan yang lebih berkesan diambil. Kecerdasan ancaman hendaklah menimbangkan perkara-perkara berikut: a. Kecerdasan ancaman strategik: pertukaran maklumat peringkat tinggi mengenai perubahan landskap ancaman (contoh: jenis penyerang atau jenis serangan); b. Kecerdasan ancaman taktikal: maklumat mengenai metodologi, alat dan teknologi penyerang terlibat; dan c. Kecerdasan ancaman operasi: perincian mengenai serangan tertentu, termasuk petunjuk teknikal.	Pentadbir Sistem Pemilik Sistem

5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK



OBJEKTIF :
Memastikan risiko keselamatan maklumat yang berkaitan dengan projek dan penghantaran ditangani dengan berkesan dalam pengurusan projek sepanjang kitaran hayat projek.

POLISI	PERANAN
KPT hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *inhouse* dan *outsource* oleh pihak luar. Kod sumber (*source code*) merupakan **HAK MILIK KPT**.	Pentadbir Sistem Pemilik Sistem

Perkara yang perlu dipatuhi adalah seperti berikut: a. Perkiraan pelesenan, kod sumber ialah HAK MILIK KPT dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara *outsource*; b. Bagi semua perkhidmatan sumber luaran dan perisian sebagai perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori "Pembekal hendaklah membenarkan Kerajaan mengakses kod sumber dan melaksanakan pengolahan risiko"; c. Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik; d. Penerimaan pengujian berdasarkan kualiti dan ketepatan serahan sistem; dan e. Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian.	

5.9 INVENTORI MAKLUMAT DAN ASET LAIN YANG BERKAITAN



OBJEKTIF:

Mengenal pasti maklumat organisasi dan aset yang berkaitan untuk dilindungi serta menetapkan pemilikan yang sesuai.

POLISI	PERANAN
Inventori maklumat dan aset hendaklah dilaksanakan seperti berikut: a. Setiap Ketua Jabatan/Bahagian/Unit hendaklah mengenal pasti Pegawai Aset di setiap Bahagian untuk menguruskan penerimaan aset-aset ICT bagi projek-projek ICT; b. Memastikan semua aset ICT dikenal pasti, diklasifikasikan, didokumentasikan, disenggarakan dan dilupuskan. Maklumat aset direkodkan dan dikemas kini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa;	Pentadbir Sistem Pegawai Aset

c. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; d. Memastikan semua perisian aplikasi dan perisian sumber ICT mempunyai lesen yang sah; e. Memastikan semua jenis aset maklumat dan ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak; dan f. Sekiranya terdapat sebarang perubahan material terhadap aset NCII selepas maklumat awal diberikan, dan perubahan tersebut memberi kesan terhadap keselamatan siber NCII atau keupayaan bertindak balas, KPT hendaklah memaklumkan secara rasmi perkara tersebut kepada Ketua Sektor NCII Kerajaan (JDN) dalam tempoh tiga puluh (30) hari dari tarikh perubahan tersebut selesai dilaksanakan.	

5.10 PENERIMAAN DAN PENGGUNAAN MAKLUMAT DAN ASET ICT



OBJEKTIF :
Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT KPT.

POLISI	PERANAN
Penerimaan dan penggunaan maklumat dan aset hendaklah dilaksanakan seperti berikut: a. Pengguna bertanggungjawab untuk melaporkan dengan SEGERA sebarang kejadian yang berkaitan keselamatan, kecurian, kehilangan atau penggunaan Aset ICT yang tidak dibenarkan; b. Aset ICT hendaklah digunakan semata-mata untuk tujuan yang berkaitan dengan perkhidmatan KPT. Ia tidak boleh dipindahkan dan dipinjamkan untuk kegunaan peribadi; c. Maklumat hendaklah dikelaskan berdasarkan keperluan undang-undang, nilai dan sensitiviti maklumat tersebut serta dilabel mengikut peringkat keselamatan maklumat;	SUB Warga KPT Pihak Ketiga

d. Media yang mengandungi maklumat perlu dilindungi; e. Memastikan maklumat yang terdapat dalam e-mel hendaklah dilindungi sebaik-baiknya; dan f. Perkara yang perlu dipertimbangkan termasuk, tetapi tidak terhad kepada, yang berikut: i. Sekatan akses yang menyokong keperluan perlindungan untuk setiap tahap klasifikasi; ii. Penyelenggaraan rekod pengguna yang dibenarkan bagi aset maklumat dan aset lain yang berkaitan; dan iii. Perlindungan salinan maklumat sementara atau kekal ke tahap yang selaras dengan perlindungan maklumat asal.	

5.11 PEMULANGAN ASET



OBJEKTIF :
Melindungi aset KPT ketika proses penukaran atau penamatan pekerjaan atau perkhidmatan kontrak.

POLISI	PERANAN
Pemulangan aset hendaklah dilaksanakan seperti berikut: a. Semua aset KPT dalam simpanan mestilah dikembalikan selepas bersara, bertukar kementerian dan penamatan perkhidmatan atau kontrak; b. Dalam tempoh notis tamat perkhidmatan dan selepas itu, organisasi hendaklah mencegah penyalinan maklumat yang tidak sah (contoh:harta intelek) oleh warga di bawah notis penamatan; c. KPT hendaklah mengenal pasti dan mendokumentasikan dengan jelas semua maklumat dan aset lain yang berkaitan yang akan dikembalikan; dan d. Aset boleh merangkumi, (tetapi tidak terhad kepada): i. Peranti pengguna (*user endpoint devices*); ii. Peranti simpanan mudah alih (*portable storage device*);	Pegawai Aset Warga KPT

iii. Peralatan pakar (*specialist equipment*); iv. Alat pengesahan (contoh: kunci mekanikal, token fizikal dan kad pintar) untuk sistem maklumat, laman web; dan v. salinan maklumat fizikal.	

5.12 KLASIFIKASI MAKLUMAT



OBJEKTIF :
Mengenal pasti kefahaman tentang keperluan perlindungan maklumat selaras dengan kepentingannya kepada organisasi.

POLISI	PERANAN
Klasifikasi maklumat hendaklah dilaksanakan seperti berikut: a. Maklumat mestilah diklasifikasikan atau dilabelkan mengikut keperluan undang-undang, nilai, tahap kritikal dan impak terhadap pendedahan atau pengubahsuaian yang tidak dibenarkan oleh pemilik maklumat yang diberi kuasa mengikut arahan keselamatan semasa. b. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan dalam dokumen Arahan Keselamatan seperti berikut: i. Terhad ii. Sulit iii. Rahsia atau iv. Rahsia besar Nota: Maklumat yang tidak dikelaskan seperti peringkat di atas diklasifikasikan sebagai maklumat “Terbuka”.	Pegawai Pengelas

5.13 PELABELAN MAKLUMAT



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

POLISI	PERANAN
Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan : a. Setiap dokumen hendaklah difailkan dan dilabelkan mengikut klasifikasi keselamatan seperti Terhad, Sulit, Rahsia atau Rahsia Besar; b. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; c. Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; d. Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti yang ditetapkan dalam Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan e. Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	Pegawai aset Pegawai Pengelas Warga KPT

5.14 PEMINDAHAN MAKLUMAT



OBJEKTIF:
Mengekalkan keselamatan maklumat yang dipindahkan dalam organisasi dan dengan mana-mana pihak luar yang berkepentingan.

POLISI	PERANAN
Memastikan keselamatan perpindahan/pertukaran data, maklumat dan perisian antara KPT dan pihak luar terjamin.	Warga KPT

Perkara yang perlu dipatuhi adalah seperti berikut: a. Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah dipatuhi untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; b. Memastikan maklumat yang terdapat dalam Mel Elektronik hendaklah dilindungi sebaik-baiknya. c. Pemindahan maklumat media storan fizikal (termasuk kertas dokumen/rekod) mestilah dilindungi melalui sebarang jenis kemudahan termasuk perkhidmatan kurier, pengangkutan dan sebagainya; d. Pemindahan maklumat secara lisan juga mesti dilindungi termasuk tidak membuat perbualan lisan sulit di tempat awam atau menggunakan komunikasi yang tidak selamat yang boleh didengari oleh orang yang tidak dibenarkan; dan e. Perjanjian hendaklah diwujudkan untuk pertukaran maklumat dan aplikasi di antara KPT dengan agensi luar.	

5.15 KAWALAN AKSES



OBJEKTIF :
Mengawal capaian yang dibenarkan dan menghalang capaian yang tidak dibenarkan kepada maklumat dan aset lain yang berkaitan.

POLISI	PERANAN
5.15.1 Akses kepada Aset ICT	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan peranan pengguna yang berbeza. a. Menentukan peraturan kawalan akses yang sesuai, hak akses dan sekatan untuk peranan pengguna tertentu terhadap aset mereka;	Pentadbir Sistem Pentadbir Rangkaian Pentadbir Pusat Data

b. Keperluan capaian hendaklah sentiasa dipantau dan dikemas kini bagi memastikan hak capaian ini diberikan kepada pegawai/pengguna yang dibenarkan sahaja; c. Sistem pengurusan kata laluan hendaklah interaktif dan mengambil kira ~~kualiti~~ kekuatan kata laluan yang dicipta; d. Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; e. Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; f. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; g. Kawalan ke atas kemudahan pemprosesan maklumat; dan h. Merekodkan semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat capaian *(Audit trail/log).*	
5.15.2 Akses kepada Internet	
Perkara-perkara berikut hendaklah dilaksanakan: a. Penggunaan internet hanyalah untuk kegunaan rasmi sahaja namun KPT berhak menentukan pengguna yang dibenarkan menggunakan internet atau sebaliknya; b. Laman yang dilayari hendaklah hanya yang berkaitan dengan semua bidang kerja dan berdasarkan Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan; c. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada pegawai yang bertanggungjawab sebelum dimuat naik ke internet;	SUB Bahagian Warga KPT Pihak Ketiga

d. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; e. Pengguna adalah dilarang melakukan aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan ii. Menyediakan, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah dan terlarang oleh undang-undang.	
5.15.3 Penggunaan Token USB	
Perkara berikut perlulah dilaksanakan : a. Token USB Kerajaan Elektronik hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; b. Token USB hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c. Perkongsian token USB untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali; dan d. Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dilaporkan.	Warga KPT

5.16 PENGURUSAN IDENTITI

OBJEKTIF :
Membenarkan pengenalan unik individu bagi mengakses sistem maklumat organisasi dan aset lain yang berkaitan serta membolehkan penyerahan hak akses yang sesuai.

POLISI	PERANAN
Perkara berikut mestilah dilaksanakan semasa pengurusan identiti pengguna: a. Akaun pengguna mestilah unik dan menggambarkan identiti pengguna; b. Akaun pengguna hendaklah diwujudkan mengikut peranan yang telah diluluskan. Sebarang perubahan terhadap capaian hendaklah mendapat kelulusan daripada pemilik sistem; c. Pemantauan akaun pengguna mestilah dilaksanakan secara berkala; dan d. Penggunaan akaun yang dikongsi bersama bagi aktiviti penambahan, pengemaskinian dan penghapusan data adalah dilarang.	SUB (BPM) Pentadbir Sistem Pentadbir e-mel

5.17 PENGESAHAN IDENTITI



OBJEKTIF :
Memastikan pengesahan entiti yang betul dan mencegah kegagalan proses pengesahan.

POLISI	PERANAN
Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh KPT seperti berikut: a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c. Panjang kata laluan mestilah sekurang-kurangnya **DUA BELAS (12) AKSARA** dengan gabungan antara huruf, aksara khas dan nombor (*alphanumeric*) **KECUALI** bagi	SUB (BPM) Warga KPT Pihak Ketiga

perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad; d. Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e. Kata laluan paparan kunci (*lock screen*) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara; g. Kuatkuasakan pertukaran kata laluan semasa atau selepas *login* kali pertama atau selepas set semula kata laluan; h. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i. Had kemasukan kata laluan bagi capaian kepada sistem aplikasi ditetapkan maksimum **TIGA (3) KALI** berturut-turut. Sekiranya cubaan melampaui had tersebut, ID capaian hendaklah **disekat secara automatik** dan hanya boleh diaktifkan semula melalui prosedur pengesahan yang ditetapkan. Walau bagaimanapun, pelaksanaan mekanisme ini adalah tertakluk kepada kekangan sistem yang diguna pakai. j. Sistem yang dibangunkan hendaklah menyediakan kemudahan untuk pengguna menukar kata laluan.	

5.18 HAK AKSES



OBJEKTIF :
Memastikan akses kepada maklumat dan aset lain yang berkaitan ditakrifkan dan dibenarkan mengikut keperluan perkhidmatan.

POLISI	PERANAN
Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong polisi kawalan capaian pengguna sedia ada. Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara–perkara berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh KPT sahaja boleh digunakan; b. Akaun pengguna mestilah unik; c. Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada KPT terlebih dahulu; d. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan e. Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan KPT.	Pentadbir Sistem Pemilik Sistem

5.19 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PEMBEKAL



OBJEKTIF :
Mengekalkan tahap keselamatan maklumat yang dipersetujui dalam pengurusan pembekal.

POLISI	PERANAN
Memastikan aset ICT KPT yang boleh dicapai oleh Pembekal dilindungi.	SUB Bahagian Pihak Ketiga

Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset KPT. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Mengenal pasti dan mendokumentasikan jenis pembekal mengikut kategori; b. Proses kitaran hayat (*lifecycle*) yang seragam untuk menguruskan pembekal; c. Mengawal dan memantau akses pembekal; d. Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian; e. Jenis-jenis obligasi kepada pembekal; f. Pelan kontingensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat; g. Pembekal perlu mematuhi Arahan Keselamatan yang berkuat kuasa; dan h. Bagi perkhidmatan pemantauan pusat operasi keselamatan terurus (SOC) dan ujian penembusan (penetration testing), penyedia perkhidmatan hendaklah merupakan penyedia yang dilesenkan secara rasmi oleh Agensi Keselamatan Siber Negara (NACSA); dan i. Bagi perkhidmatan juruaudit di bawah Akta 854, kelulusan pelantikan daripada Ketua Eksekutif NACSA hendaklah diperoleh sebelum audit dilaksanakan. Laporan Audit Keselamatan Siber hendaklah dihantar ke NACSA dan JDN dalam tempoh 30 hari selepas audit dan juruaudit mesti menandatangani Perjanjian Kerahsiaan (NDA) dengan pihak KPT; dan j. Menandatangani **Surat Akuan Pematuhan PKS KPT**	

5.20 MENANGANI KESELAMATAN MAKLUMAT DI DALAM PERJANJIAN PEMBEKAL



OBJEKTIF :
Mengekalkan tahap keselamatan maklumat yang dipersetujui dalam pengurusan pembekal.

POLISI	PERANAN
a. Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi; b. Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak KPT selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa; c. Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut: i. KPT hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan; ii. Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan; iii. Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan;	SUB (BPM) Pihak ketiga

iv. Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; v. Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian melalui laporan yang dikemukakan oleh syarikat pembekal; vi. Laporan penilaian yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut: (a) Badan penilai pembekal adalah bebas dan berintegriti; (b) Badan penilai pembekal adalah kompeten; (c) Kriteria penilaian; (d) Parameter pengujian; dan (e) Andaian yang dibuat berkaitan dengan skop penilaian. vii. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan KPT; dan viii. Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh KPT.	

5.21 MENGURUSKAN KESELAMATAN MAKLUMAT DALAM RANTAIAN BEKALAN ICT



OBJEKTIF :
Mengekalkan tahap keselamatan maklumat yang dipersetujui dalam hubungan pembekal.

POLISI	PERANAN
Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan ICT serta rantaian bekalan produk. Perkara-perkara yang perlu diambil kira adalah seperti berikut:	SUB (BPM) Pihak Ketiga

a. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b. Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada kontraktor atau pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan c. Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	

5.22 MEMANTAU, MENGKAJI DAN PENGURUSAN PERUBAHAN PERKHIDMATAN PEMBEKAL



OBJEKTIF :
Mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal.

POLISI	PERANAN
KPT hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a. Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; b. Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan c. Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian. d. Perubahan kepada peruntukan perkhidmatan oleh pembekal termasuk mempertahankan dan menambah baik polisi keselamatan maklumat sedia ada, prosedur dan kawalan hendaklah diuruskan dengan mengambil	SUB Bahagian Pihak Ketiga

kira kepentingan maklumat, sistem dan proses bisnes yang terlibat serta penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti berikut: i. Perubahan dalam perjanjian dengan pembekal; ii. Perubahan yang dilakukan oleh KPT bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian polisi dan prosedur; dan iii. Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baharu, produk-produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	

5.23 KESELAMATAN MAKLUMAT UNTUK PENGGUNAAN PERKHIDMATAN AWAN



OBJEKTIF :
Memastikan pengurusan keselamatan maklumat yang berkesan bagi penggunaan perkhidmatan awan.

POLISI	PERANAN
Untuk memastikan keselamatan maklumat dalam menggunakan perkhidmatan awan, beberapa langkah kawalan utama perlu diambil kira. KPT perlu memastikan : a. Penilaian pemilihan pengkomputeran awan hendaklah dibuat secara terperinci berdasarkan keperluan, pematuhan kepada dasar sedia ada dan kekangan undang-undang yang berkaitan sebelum sebarang keputusan untuk menggunakan perkhidmatan pengkomputeran awan dibuat; b. KPT hendaklah memastikan kandungan kontrak perjanjian seperti *Customer Agreement, Service Level Agreement* (SLA) atau *Acceptable Use Policy* (AUP), termasuk klausa keselamatan maklumat dan perlindungan data, difahami sebelum menggunakan sebarang perkhidmatan awan;	SUB(BPM) ICTSO

c. Data atau maklumat yang terdapat di pengkomputeran awan adalah milik penuh KPT dan hanya boleh diakses oleh pihak yang diberikan kebenaran; dan d. Klausa berkaitan dengan pelucutan pentauliahan atau menamatkan kontrak hendaklah dinyatakan dengan jelas dalam kontrak perjanjian bersama CSP (*Cloud Service Provider*). Memastikan tatacara perkhidmatan pengkomputeran awan yang dilaksanakan mematuhi peraturan yang sedang berkuat kuasa.	

5.24 PELAN DAN PENYEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT



OBJEKTIF :
Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi tentang kejadian dan kelemahan keselamatan.

POLISI	PERANAN
Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan insiden KPT adalah berdasarkan Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT KPT yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memberikan kesedaran berkaitan Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT KPT dan hebahan kepada Warga KPT sekiranya ada perubahan;	ICTSO CSIRT BKP

b. Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan; c. Maklumat mengenai insiden keselamatan yang dikendalikan hendaklah disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada KPT; d. Bahan-bahan bukti berkaitan insiden keselamatan hendaklah disimpan dan disenggarakan; dan e. Kawalan keselamatan hendaklah mengambil kira perkara berikut: i. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; ii. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; iii. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; iv. Menyediakan tindakan pemulihan segera; dan v. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu. f. Bagi Insiden Keselamatan kategori NCII, hendaklah mengambil tindakan berikut: i. Individu yang diberi kuasa oleh KPT hendaklah dengan serta-merta memberitahu insiden keselamatan siber yang telah atau mungkin berlaku melalui e-mel rasmi NACSA (*cert@nc4.gov.my*). ii. Dalam tempoh enam (6) jam dari masa insiden keselamatan siber diketahui, individu yang diberi kuasa hendaklah mengemukakan maklumat yang diperlukan melalui portal NC4 (*www.nc4.gov.my*) iii. Dalam tempoh empat belas (14) hari selepas pemberitahuan awal, individu yang diberi kuasa hendaklah menyediakan maklumat tambahan sepenuhnya di Portal NC4.	

5.24.2 Mekanisme pelaporan	
a. Insiden keselamatan maklumat seperti berikut hendaklah dilaporkan kepada CSIRT dengan kadar segera: b. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau disyaki hilang atau didedahkan kepada pihak-pihak yang tidak dibenarkan; c. Sistem maklumat (ICT) digunakan tanpa kebenaran atau disyaki sedemikian; d. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; e. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan f. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Rujuk Prosedur pelaporan insiden keselamatan ICT berdasarkan: a. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan b. Surat Pekeliling Am Bilangan 4 Tahun 2022, Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam.	ICTSO CSIRT Warga KPT

5.25 PENILAIAN DN KEPUTUSAN INSIDEN KESELAMATAN MAKLUMAT



OBJEKTIF :
Memastikan pengkategorian dan keutamaan insiden keselamatan maklumat yang berkesan.

POLISI	PERANAN
Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat. Penilaian dan keputusan mengenai insiden keselamatan maklumat hendaklah dilaksanakan seperti berikut: a. Maklumat insiden keselamatan mestilah dinilai dan diputuskan; dan b. Keputusan penilaian hendaklah direkodkan secara terperinci untuk tujuan pengesahan dan rujukan pada masa hadapan.	CSIRT ICTSO BKP

5.26 TINDAKBALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT



OBJEKTIF :
Memastikan tindak balas yang cekap dan berkesan terhadap insiden keselamatan maklumat.

POLISI	PERANAN
a. Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan Prosedur Pengendalian Insiden Keselamatan; b. Menyelaras dengan pihak dalaman dan luaran seperti pihak berkuasa, kumpulan kepentingan luaran dan forum, pembekal dan pelanggan untuk meningkatkan keberkesanan tindak balas dan membantu meminimumkan akibat bagi organisasi lain; dan c. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: i. Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; ii. Menjalankan kajian forensik sekiranya perlu;	ICTSO CSIRT BKP Pentadbir Sistem Pemilik Sistem

iii. Menghubungi pihak yang berkenaan dengan secepat mungkin; iv. Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti; v. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; vi. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; vii. Menyediakan tindakan pemulihan segera; dan viii. Memaklumkan atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	

5.27 PENGAJARAN DARI INSIDEN KESELAMATAN MAKLUMAT



OBJEKTIF :
Mengurangkan kemungkinan atau akibat insiden masa hadapan

POLISI	PERANAN
a. Pengetahuan yang diperoleh daripada penganalisisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya; dan b. Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah. c. Mengenal pasti kejadian berulang atau serius dan penyebabnya untuk mengemas kini pentaksiran risiko keselamatan maklumat organisasi dan menentukan dan melaksanakan kawalan tambahan yang diperlukan untuk mengurangkan kemungkinan atau akibat kejadian serupa pada masa hadapan. Mekanisme untuk membolehkannya merangkumi pengumpulan, pengukuran dan pemantauan maklumat mengenai jenis, jumlah dan kos kejadian; d. Meningkatkan kesedaran dan latihan kepada pengguna (rujuk 6.3) dengan memberikan contoh apa yang boleh berlaku, bagaimana bertindak balas terhadap insiden	ICTSO CSIRT KPT Pemilik Sistem BKP

tersebut dan bagaimana menghindarinya pada masa hadapan.	

5.28 PENGUMPULAN BUKTI



OBJEKTIF :
Memastikan pengurusan bukti yang konsisten dan berkesan berkaitan insiden keselamatan maklumat bagi mengambil tindakan tatatertib dan undang-undang.

POLISI	PERANAN
KPT hendaklah menentukan prosedur bagi pengenalpastian, pengumpulan, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pasukan tindak balas insiden mesti mendokumentasikan dengan jelas bahan bukti yang akan dipelihara, termasuk sistem yang telah dikompromi. Semua bahan bukti harus dikumpul mengikut prosedur yang menepati undang-undang dan peraturan supaya boleh diterima pakai di mahkamah atau mana-mana forum disiplin keselamatan maklumat; dan b. Log yang terperinci mesti disimpan bagi setiap bahan bukti. Semua log mesti disenggara, disemak dan diawasi.	ICTSO CSIRT BKP

5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN



OBJEKTIF :
Melindungi maklumat dan aset lain yang berkaitan semasa gangguan.

POLISI	PERANAN
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes, impak gangguan yang mungkin berlaku dan kesannya terhadap keselamatan siber serta tindakan bagi meminimumkan impak gangguan tersebut; b. Melaksanakan prosedur tindak balas kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; c. Mendokumentasikan proses dan prosedur yang telah dipersetujui; d. Mengadakan program latihan mengenai prosedur kecemasan; e. Membuat *backup* mengikut keperluan DRP; dan f. Pelan DRP hendaklah diuji sekurang-kurangnya setahun sekali atau apabila terdapat keperluan.	SUB (BPM) CSIRT KPT Warga KPT Pihak Ketiga

5.30 KESEDIAAN ICT UNTUK KESINAMBUNGAN PERKHIDMATAN



OBJEKTIF :
Memastikan ketersediaan maklumat organisasi dan aset lain yang berkaitan semasa gangguan.

POLISI	PERANAN
Perkara berikut hendaklah dilaksanakan: a. Pelan Pemulihan Bencana (DRP) dan Pelan Kesinambungan Perkhidmatan (PKP) hendaklah dibangunkan, didokumenkan, dan diselenggara secara berterusan bagi memastikan kelangsungan serta ketersediaan perkhidmatan ICT KPT	ICTSO SUB(BPM)

terutamanya semasa berlaku gangguan atau bencana; b. Pengujian dan simulasi DRP serta PKP hendaklah dilaksanakan secara berkala sekurang-kurangnya sekali setahun atau mengikut keperluan semasa. c. Pengurusan kesinambungan perkhidmatan ICT KPT hendaklah sentiasa dijajarkan dan mematuhi pekeliling, garis panduan, piawaian, serta arahan keselamatan siber dan pengurusan bencana nasional yang berkuat kuasa.	

5.31 KEPERLUAN UNDANG-UNDANG, KANUN, PERATURAN DAN KONTRAK



OBJEKTIF :
Memastikan pematuhan kepada keperluan undang-undang berkanun, peraturan dan kontrak yang berkaitan dengan keselamatan maklumat.

POLISI	PERANAN
a. Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh Warga KPT, Pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT; b. Keperluan luaran termasuk keperluan undang-undang, kanun, peraturan atau kontrak hendaklah dipertimbangkan (tetapi tidak terhad kepada) semasa; i. Membangun/ menyemak polisi dan prosedur keselamatan maklumat; ii. Merancang, melaksanakan atau mengubah kawalan keselamatan maklumat; iii. Mengklasifikasikan maklumat dan aset lain yang berkaitan sebagai sebahagian daripada proses untuk menetapkan keperluan keselamatan maklumat untuk keperluan dalaman atau untuk perjanjian pembekal;	Warga KPT Pihak Ketiga

iv. Melakukan penilaian risiko keselamatan maklumat dan menentukan aktiviti rawatan risiko keselamatan maklumat; v. Menentukan proses bersama dengan peranan dan tanggungjawab yang berkaitan dengan keselamatan maklumat; dan vi. Menentukan keperluan kontrak pembekal yang berkaitan dengan organisasi dan skop pembekalan produk dan perkhidmatan.	

5.32 HAK HARTA INTELEK



OBJEKTIF :
Memastikan pematuhan terhadap keperluan undang-undang, berkanun, peraturan dan kontrak yang berkaitan dengan hak harta intelek dan penggunaan produk proprietari.

POLISI	PERANAN
a. Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual; b. Melaksanakan kawalan terhadap keperluan pelesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had Pengguna yang telah ditetapkan atau dibenarkan; dan c. Hak harta intelek bagi program perisian, dokumentasi dan maklumat lain yang dijana oleh atau disediakan oleh pengguna dan pembekal KPT mestilah menjadi hak milik KPT/ Kerajaan.	Warga KPT Pihak Ketiga

5.33 PERLINDUNGAN REKOD



OBJEKTIF :
Memastikan pematuhan kepada keperluan undang-undang, berkanun, peraturan dan kontrak, serta kepentingan komuniti atau masyarakat yang berkaitan dengan perlindungan dan ketersediaan rekod.

POLISI	PERANAN
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap rekod perlu dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian dan pembebasan yang tidak dibenarkan, mengikut keperluan perundangan, peraturan, kontrak dan perkhidmatan; dan b. Tandatangan digital hanya boleh digunakan untuk surat rasmi atau memo yang diklasifikasikan sebagai terbuka dan terhad sahaja.	Warga KPT Pihak Ketiga

5.34 PRIVASI DAN PELINDUNGAN MAKLUMAT PENGENALAN PERIBADI (PII)



OBJEKTIF :
Memastikan pematuhan kepada keperluan undang-undang, berkanun, peraturan dan kontrak yang berkaitan dengan aspek keselamatan maklumat perlindungan PII.

POLISI	PERANAN
KPT hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti yang ditetapkan dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.	CDO SUB Bahagian

5.35 KAJIAN BEBAS KESELAMATAN MAKLUMAT



OBJEKTIF :
Memastikan kesesuaian, kecukupan dan keberkesanan berterusan pendekatan organisasi untuk mengurus risiko keselamatan maklumat.

POLISI	PERANAN
a. Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur; dan b. Perkara-perkara berikut hendaklah dipertimbangkan (tetapi tidak terhad kepada): i. Undang-undang dan peraturan yang mempengaruhi perubahan organisasi; ii. Insiden ketara berlaku; dan iii. Terdapat perubahan dalam perkhidmatan, arahan, prosedur keselamatan maklumat atau yang setara dengannya. c. Audit berhubung keselamatan siber oleh NACSA hendaklah dijalankan sekurang-kurangnya sekali dalam tiap-tiap dua tahun bermula dari tarikh penetapan sebagai entiti NCII, oleh juruaudit yang mendapat kelulusan Ketua Eksekutif NACSA; dan d. Dapatan Audit berserta pelan tindakan pembetulan hendaklah dikemukakan kepada Ketua Eksekutif NACSA (melalui *auditpematuhan@nacsa.gov.my*) dan disalinkan kepada Ketua Sektor NCII Kerajaan JDN (melalui *ncii@jdn.gov.my*) dalam tempoh 30 hari dari tarikh selesai audit dilaksanakan.	SUB (BPM)

5.36 PEMATUHAN DENGAN POLISI, PERATURAN DAN PIAWAIAN UNTUK KESELAMATAN MAKLUMAT



OBJEKTIF :
Memastikan keselamatan maklumat dilaksanakan dan dikendalikan mengikut Polisi Keselamatan Siber organisasi, prosedur, peraturan dan standard yang ditetapkan.

POLISI	PERANAN
	SUB Bahagian

a. KPT hendaklah membuat kajian semula secara berkala terhadap pematuhan polisi dan standard keselamatan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan polisi, piawaian dan keperluan teknikal yang bersesuaian; dan b. Prosedur sistem maklumat ICT yang dilaksanakan mestilah sentiasa disemak untuk mematuhi Polisi Keselamatan Siber organisasi dan standard yang bersesuaian.	SUB(BPM)

5.37 PROSEDUR OPERASI YANG DIDOKUMENKAN



OBJEKTIF :
Memastikan operasi yang betul dan selamat bagi sistem dan fasiliti pemprosesan maklumat ICT serta pemprosesan maklumat perkhidmatan organisasi.

POLISI	PERANAN
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur keselamatan ICT yang diwujudkan, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b. Semua prosedur hendaklah dikemas kini dari masa ke semasa atau mengikut keperluan; dan c. Semua kakitangan KPT hendaklah mematuhi prosedur yang telah ditetapkan.	SUB BPM

5.38 PENGGUNAAN TEKNOLOGI KECERDASAN BUATAN (AI)



OBJEKTIF :
Memastikan penggunaan dan pengadaptasian teknologi Kecerdasan Buatan (*Artificial Intelligence* – AI) di KPT dilaksanakan secara selamat, bertanggungjawab dan beretika serta tidak menjejaskan keselamatan maklumat dan aset ICT KPT.

POLISI	PERANAN
Penggunaan teknologi AI termasuk AI Generatif (*Generative AI*) bagi urusan rasmi KPT hendaklah dilaksanakan secara terkawal dengan mengambil kira aspek keselamatan maklumat, perlindungan data, privasi, ketepatan maklumat, akauntabiliti dan pengurusan risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan teknologi AI hendaklah mematuhi perundangan, dasar, arahan, pekeliling dan garis panduan Kerajaan yang berkuat kuasa; b. Maklumat yang dimasukkan, dimuat naik atau diproses melalui teknologi AI hendaklah mematuhi keperluan klasifikasi dan perlindungan maklumat KPT; c. Maklumat Rahsia Rasmi, maklumat terperingkat atau apa-apa maklumat yang dilindungi tidak boleh dimasukkan ke dalam aplikasi atau perkhidmatan AI yang tidak dibenarkan oleh KPT; d. Output yang dihasilkan oleh AI hendaklah disemak dan disahkan sewajarnya sebelum digunakan bagi tujuan rasmi KPT; e. Penggunaan AI tidak menghapuskan tanggungjawab dan akauntabiliti pegawai terhadap keputusan, tindakan atau dokumen yang dihasilkan dengan bantuan AI; f. Penggunaan atau pengadaptasian AI hendaklah mengambil kira risiko keselamatan siber dan risiko	CDO ICTSO SUB(BPM) Pemilik Sistem Warga KPT Pihak Ketiga

terhadap kerahsiaan, integriti serta ketersediaan maklumat dan perkhidmatan KPT; dan g. Tatacara penggunaan dan pengadaptasian AI hendaklah merujuk kepada Garis Panduan Pengadaptasian Kecerdasan Buatan (AI) Sektor Awam, Jabatan Digital Negara (JDN) serta apa-apa arahan atau garis panduan Kerajaan berkaitan AI yang berkuat kuasa dari semasa ke semasa.	

KAWALAN

KESELAMATAN MANUSIA

KAWALAN KESELAMATAN ORGANISASI MERANGKUMI PERATURAN DAN LANGKAH YANG MENETUKAN SIKAP KOMPREHENSIF ORGANISASI TERHADAP PERLINDUNGAN DATA DALAM PELBAGAI PERKARA. KAWALAN INI TERMASUK POLISI, PERATURAN, PROSES, PROSEDUR, STRUKTUR ORGANISASI DAN SEBAGAINYA



6.1 SARINGAN



OBJEKTIF :
Memastikan semua pengguna KPT dapat melaksanakan peranan dan tanggungjawab melalui penilaian keselamatan atas kelayakan dan kesesuaian semasa bekerja.

POLISI	PERANAN
Memastikan Warga KPT, Pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT KPT memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Tapisan keselamatan hendaklah dijalankan terhadap Warga KPT, pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT KPT yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab Warga KPT, Pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT KPT yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan b. Menjalankan tapisan keselamatan untuk Warga KPT, Pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT KPT yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	SUB Bahagian Warga KPT Pihak Ketiga

6.2 TERMA DAN SYARAT PERKHIDMATAN



OBJEKTIF:
Memastikan semua pengguna KPT memahami tanggungjawab keselamatan maklumat mereka bagi peranan yang dipertimbangkan untuk mereka.

POLISI	PERANAN
Persetujuan berkontrak dengan Warga KPT, Pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT KPT hendaklah menyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut: a. Menyatakan dengan lengkap dan jelas peranan serta tanggungjawab Warga KPT, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPT yang terlibat dalam menjamin keselamatan aset ICT; dan b. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	SUB Bahagian Warga KPT Pihak ketiga

6.3 KESEDARAN, PENDIDIKAN DAN LATIHAN KESELAMATAN MAKLUMAT



OBJEKTIF :
Memastikan semua pengguna KPT dan pihak berkepentingan yang berkaitan memenuhi tanggungjawab terhadap keselamatan maklumat dan privasi di organisasi.

POLISI	PERANAN
Warga KPT, Pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT KPT perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan kesedaran, pendidikan dan latihan yang berkaitan PKS KPT, Sistem Pengurusan Keselamatan	ICTSO

Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka; b. Memastikan kesedaran yang berkaitan PKS KPT perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan c. Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.	

6.4 PROSES TATATERTIB



OBJEKTIF :
Memastikan warga KPT dan pihak berkepentingan lain memahami akibat pelanggaran Polisi Keselamatan Siber dan privasi bagi mencegah pelanggaran serta memastikan tindakan sewajarnya diambil terhadap pihak yang melakukan pelanggaran tersebut.

POLISI	PERANAN
Proses tatatertib yang formal dan disampaikan kepada Warga KPT hendaklah tersedia bagi membolehkan tindakan diambil terhadap Warga KPT yang melakukan pelanggaran keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas Warga KPT sekiranya berlaku pelanggaran terhadap perundangan dan peraturan yang ditetapkan oleh KPT; dan b. Warga KPT yang melanggar polisi ini akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT KPT.	KSU

6.5 PENAMATAN ATAU PERTUKARAN JAWATAN



OBJEKTIF:
Memastikan pertukaran, tamat perkhidmatan dan perubahan bidang tugas Warga KPT diurus dengan teratur.

POLISI	PERANAN
Warga KPT yang bertukar atau tamat perkhidmatan hendaklah: a. Memastikan semua aset ICT dikembalikan kepada KPT mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; b. Memaklumkan kepada Pentadbir Sistem untuk pembatalan semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan KPT dan/atau terma perkhidmatan yang ditetapkan; dan c. Menyediakan dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.	SUB Bahagian Pentadbir Sistem SUB(BPM) Warga KPT

6.6 PERJANJIAN KERAHSIAAN ATAU KETERDEDAHAN



OBJEKTIF :
Mengekalkan kerahsiaan maklumat yang boleh diakses oleh warga KPT atau pihak ketiga.

POLISI	PERANAN
a. Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan didokumentasikan; dan b. Pihak Ketiga hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.	SUB (BPM) Pemilik Sistem Pihak Ketiga Warga KPT

6.7 TELEKERJA (REMOTE WORKING)



OBJEKTIF:
Untuk memastikan keselamatan maklumat apabila pengguna bekerja dari jauh.

POLISI	PERANAN
a. Polisi dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi telekerja; b. Kawalan capaian dijalankan bergantung pada kategori Pengguna, sensitiviti aplikasi dan jenis data yang dicapai dan tetapan mudah alih dan telekerja; dan c. Capaian maklumat dan aplikasi di pusat data melalui jarak jauh (*remote access*) adalah terhad kepada Pengguna yang dibenarkan sahaja dan mestilah melalui *Virtual Private Network* (VPN).	Warga KPT

6.8 PELAPORAN INSIDEN KESELAMATAN MAKLUMAT



OBJEKTIF:
Menyokong pelaporan tepat pada masanya, konsisten dan berkesan tentang insiden keselamatan maklumat yang boleh dikenal pasti oleh pengguna.

POLISI	PERANAN
a. Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan ICT atau ancaman yang berlaku hendaklah dilaporkan kepada CSIRT KPT. CSIRT KPT kemudiannya perlu melaporkan kepada ICTSO dengan kadar segera. b. Perkara yang perlu dipertimbangkan adalah seperti berikut:	SUB (BPM) CSIRT Pemilik Sistem Warga KPT

i. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa; ii. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; iii. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan; iv. Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau didedahkan; v. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan vi. Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka. c. Prosedur Pelaporan insiden keselamatan siber bagi aset yang dikategorikan sebagai NCII hendaklah selaras dengan Akta 854 manakala pelaporan bagi Insiden yang bukan dikategorikan sebagai NCII adalah berdasarkan tatacara dan pekeliling semasa yang berkuat kuasa.	

KAWALAN

KESELAMATAN FIZIKAL

KAWALAN KESELAMATAN FIZIKAL MERUPAKAN PERLINDUNGAN FIZIKAL UNTUK MEMASTIKAN KESELAMATAN ASET KETARA. INI TERMASUK PROSES AKSES PENGGUNA, PROSES PELUPUSAN ASET, PROSES MEDIUM SOTAN DAN POLISI MEJA BERSIH DAN SKRIN KOSONG.



7.1 PERIMETER KESELAMATAN FIZIKAL



OBJEKTIF :
Menghalang akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat KPT.

POLISI	PERANAN
Ini bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan aset ICT KPT. Perkara-perkara yang perlu dipatuhi seperti berikut: a. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; b. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; c. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; d. Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan manusia; e. Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; f. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada kemasukan pihak yang tidak diberi kebenaran memasukinya; dan g. Memasang alat penggera atau kamera keselamatan.	SUB (BKP) ICTSO Pentadbir Pusat Data

7.2 KEMASUKAN FIZIKAL



OBJEKTIF :
Memastikan hanya akses fizikal yang dibenarkan kepada maklumat organisasi dan aset lain yang berkaitan.

POLISI	PERANAN
Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis KPT. Perkara yang perlu dipatuhi adalah seperti berikut: a. Warga KPT hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan kepada KPT apabila bertukar, tamat perkhidmatan atau bersara; b. Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan serta mengembalikan pas tersebut selepas tamat lawatan; c. Hanya Pengguna yang diberi kebenaran sahaja boleh menggunakan aset ICT KPT; d. Kehilangan pas keselamatan hendaklah dilaporkan segera kepada Pihak Berkuasa; e. Kawasan larangan di KPT ialah Pusat Data (*Data Centre*). Akses kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; f. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali diberikan kebenaran bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal dan mereka hendaklah diiringi masuk oleh pegawai-pegawai yang dibenarkan ke dalam kawasan berkenaan; dan g. Buku log hendaklah disediakan bagi merekodkan maklumat pihak ketiga yang memasuki kawasan larangan.	SUB (BKP) Warga KPT PentadbirPusat Data

7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN (FASILITI)



OBJEKTIF:
Mengelakkan akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada maklumat organisasi dan aset lain yang berkaitan di pejabat, bilik dan kemudahan.

POLISI	PERANAN
Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Kawasan tempat bekerja, bilik mesyuarat, bilik krisis, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan *Closed-Circuit Television* (CCTV) dan pusat data perlu dihadkan daripada diakses tanpa kebenaran; b. Kawasan tempat bekerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar; dan c. Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi Arahan Keselamatan.	SUB Bahagian SUB (BKP) Warga KPT

7.4 PEMANTAUAN KESELAMATAN FIZIKAL



OBJEKTIF:
Mengesan dan menghalang akses fizikal yang tidak dibenarkan.

POLISI	PERANAN
Tujuan utama kawalan ini adalah untuk mengesan, merekodkan, dan memberi amaran mengenai aktiviti-aktiviti yang mencurigakan yang boleh menjejaskan keselamatan aset fizikal dan maklumat. Ini dapat membantu mengurangkan risiko kehilangan atau kerosakan aset serta memastikan keselamatan dan kesejahteraan KPT. Berikut merupakan perkara yang perlu dipatuhi :	SUB (BKP)

a. Menggunakan kamera pengawasan untuk memantau kawasan-kawasan kritikal seperti pintu masuk, ruang pelayan, bilik kawalan dan mana-mana kawasan yang dikategorikan kritikal. Kamera pengawasan hendaklah diletakkan di tempat yang strategik untuk mendapatkan liputan yang maksimum; b. Memasang sistem penggera yang akan berbunyi apabila terdapat cubaan untuk memasuki kawasan larangan; c. Menggunakan kad akses/sistem biometrik untuk mengawal pegawai atau pelawat yang boleh memasuki kawasan tertentu. Setiap pergerakan keluar masuk haruslah direkodkan; d. Melaksanakan rondaan secara berkala oleh pengawal keselamatan untuk memastikan setiap kawasan selamat. Merekodkan dan melaporkan kejadian kepada penyelia; e. Menggunakan teknologi yang membolehkan pemantauan keselamatan fizikal secara jarak jauh; f. Menubuhkan pusat kawalan keselamatan yang berfungsi sebagai pusat operasi untuk memantau semua aktiviti keselamatan fizikal; g. Mematuhi prosedur tindak balas insiden yang berkuat kuasa untuk memastikan tindakan segera diambil apabila terdapat pelanggaran keselamatan; h. Melaksanakan audit keselamatan fizikal secara berkala untuk memastikan semua sistem dan prosedur berfungsi dengan baik; dan i. Melaksanakan latihan kepada Warga KPT mengenai prosedur keselamatan fizikal dan cara menggunakan peralatan keselamatan.	

7.5 PERLINDUNGAN DARIPADA ANCAMAN LUAR DAN PERSEKITARAN



OBJEKTIF:
Mencegah atau mengurangkan akibat kejadian yang berpunca daripada ancaman fizikal dan alam sekitar.

POLISI	PERANAN
a. Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. KPT perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan pergolakan awam; b. Prosedur perlindungan peralatan ICT daripada ancaman fizikal dan alam sekitar mestilah dilaksanakan seperti berikut (tetapi tidak terhad kepada): i. Peralatan ICT yang berada di Pusat Data mesti diletakkan dengan sewajarnya dan dilindungi daripada ancaman dan bahaya alam sekitar (contoh: kebakaran, asap, banjir, habuk, gangguan bekalan elektrik) dan akses tanpa kebenaran (contoh: kecurian) untuk memastikan peralatan berterusan dalam operasi; dan ii. Semua peralatan ICT mesti diselenggara secara berkala mengikut spesifikasi kawalan keselamatan yang disyorkan oleh pembekal. c. Mematuhi prosedur insiden kecemasan yang ditetapkan; dan d. Melaporkan insiden kecemasan persekitaran seperti kebakaran.	SUB (BKP) SUB (BPM) Warga KPT

7.6 BEKERJA DIKAWASAN SELAMAT



OBJEKTIF:
Melindungi maklumat dan aset yang berkaitan di pejabat dan kawasan selamat daripada kerosakan dan gangguan oleh pengguna lain.

POLISI	PERANAN
a. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi Warga KPT yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis KPT termasuklah Pusat Data. b. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. c. Kawalan keselamatan ke atas kawasan tersebut adalah seperti berikut: i. Sumber data atau pelayan, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik pelayan atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran; ii. Akses adalah terhad kepada Warga KPT yang telah diberi kuasa sahaja dan dipantau pada setiap masa; iii. Pemantauan dibuat menggunakan kamera *Closed-Circuit Television* (CCTV) atau peralatan lain yang sesuai; iv. Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual; v. Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; vi. Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab sepanjang tempoh di lokasi berkaitan; vii. Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam; viii. Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan; ix. Memperkukuh dinding dan siling; dan	SUB (BKP)

x. Mengehadkan jalan keluar masuk.	

7.7 MEJA BERSIH DAN SKRIN KOSONG (CLEAR DESK AND CLEAR SCREEN)



OBJEKTIF:
Mengurangkan risiko akses tanpa kebenaran, kehilangan dan kerosakan maklumat pada meja, skrin dan di lokasi lain yang boleh diakses semasa dan di luar waktu kerja biasa.

POLISI	PERANAN
a. Polisi meja kosong untuk kertas dan media penyimpanan boleh alih serta polisi skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan. b. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. c. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada atas meja Pengguna atau di paparan skrin apabila Pengguna tidak berada di tempatnya. d. Langkah-langkah yang perlu diambil termasuklah seperti berikut: i. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; ii. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; iii. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat; iv. E-mel masuk dan keluar hendaklah dikawal; dan v. Menghalang Penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.	Warga KPT Pihak Ketiga

7.8 PERLINDUNGAN PERALATAN



OBJEKTIF:
Mengurangkan risiko peralatan daripada ancaman fizikal dan alam sekitar, kerosakan dan akses yang tidak dibenarkan.

POLISI	PERANAN
Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; b. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c. Pengguna dilarang sama sekali menambah, menanggalkan atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d. Pengguna dilarang memasang sebarang perisian tambahan tanpa kebenaran; e. Pengguna mesti memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; f. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, pengubahsuaian tanpa kebenaran dan penyalahgunaan; g. Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya;	SUB(BPM) Pentadbir Sistem Pemilik Sistem Pentadbir Pusat Data Pentadbir Rangkaian Warga KPT UKTN

h. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptible Power Supply* (UPS) dan *Generator Set* (*Gen-Set*); i. Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; j. Peralatan rangkaian seperti suis, penghala, hab dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci; k. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; l. Peralatan ICT yang hendak dibawa ke luar premis KPT, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan; m. Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden; n. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; o. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pentadbir Sistem ICT; p. Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih; q. Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; r. Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal;	

s. Pengguna dilarang sama sekali mengubah ***password administrator*** yang telah ditetapkan oleh pihak ICT; dan t. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi dan KPT sahaja.	

7.9 KESELAMATAN ASET LUAR PREMIS



OBJEKTIF:
Mengelakkan kehilangan, kerosakan, kecurian atau kompromi peranti luar tapak dan gangguan kepada operasi organisasi.

POLISI	PERANAN
Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis KPT. Peralatan yang dibawa keluar dari premis KPT adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti berikut: a. Peralatan perlu dilindungi dan dikawal sepanjang masa; b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan c. Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.	Warga KPT Pihak Ketiga

7.10 MEDIA STORAN



OBJEKTIF:
Memastikan hanya pendedahan yang dibenarkan, pengubahsuaian, penyingkiran atau pemusnahan maklumat pada media storan.

POLISI	PERANAN
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Prosedur hendaklah dilaksanakan bagi pengurusan media storan menurut kaedah arahan keselamatan; b. Media storan hendaklah dilupuskan dengan selamat berdasarkan tatacara/ pekeliling semasa yang berkuat kuasa; dan c. Media storan yang mengandungi maklumat hendaklah dilindungi daripada capaian tanpa izin, penyalahgunaan atau kerosakan semasa proses pengangkutan.	Warga KPT
7.10.1 Peranti tandatangan Digital (*Digital Signature Device*)	
Peranti Tandatangan Digital merupakan peranti fizikal yang dilindungi kata laluan yang digunakan bagi melindungi identiti peribadi. Tandatangan digital dikaitkan dengan penandatangan membuat transaksi dokumen secara selamat. (Contoh: *Public Key Infrastructure* (PKI) dan Token USB, kad memori). Perkara-perkara berikut hendaklah dilaksanakan: a. Bertanggungjawab sepenuhnya melindungi peranti tandatangan digital daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b. Peranti ini tidak boleh dipindah milik atau dipinjamkan; c. Penyedia perkhidmatan tandatangan digital yang dilantik hendaklah mengenakan pengesahan dua faktor (*dual-factor authentication*) sebelum dokumen boleh ditandatangani oleh pengguna. Kaedah pengesahan yang digunakan juga berbeza-beza (contoh: menghantar kata laluan sekali sahaja melalui SMS dan pengimbasan biometrik pada telefon mudah alih); dan	Warga KPT

d. Sebarang insiden kehilangan peranti ini hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	

7.11 UTILITI SOKONGAN



OBJEKTIF:
Mengelakkan kehilangan, kerosakan atau kompromi maklumat dan aset lain yang berkaitan, atau gangguan kepada operasi organisasi akibat kegagalan dan gangguan utiliti sokongan.

POLISI	PERANAN
a. KPT hendaklah mengelakkan risiko kepada ketersediaan dan integriti aset maklumat akibat kegagalan utiliti sokongan seperti gas, penyaman udara, telekomunikasi, air dan elektrik. b. Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan; dan c. Semua alat sokongan perlu disenggara dari semasa ke semasa secara berkala.	SUB (BKP)

7.12 KESELAMATAN KABEL



OBJEKTIF:
Mengelakkan kehilangan, kerosakan, kecurian atau kompromi maklumat dan aset lain yang berkaitan dan gangguan kepada operasi organisasi yang berkaitan dengan kabel kuasa dan komunikasi.

POLISI	PERANAN
Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Kabel	Pentadbir Rangkaian SUB (BKP)

termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan d. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	SUB(BPM)

7.13 PENYELENGGARAAN PERALATAN



OBJEKTIF:
Mengelakkan kehilangan, kerosakan, kecurian atau kompromi maklumat dan aset yang berkaitan yang mengakibatkan gangguan kepada operasi organisasi yang disebabkan oleh kelemahan penyelenggaraan.

POLISI	PERANAN
a. Peralatan ICT hendaklah disenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. b. Perkakasan hendaklah disenggara dengan betul bagi memastikan ketersediaan, kerahsiaan dan integriti. c. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: i. Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama	SUB (BPM) SUB (BKP) Pentadbir Sistem

ada dalam tempoh jaminan atau telah habis tempoh jaminan; ii. Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; iii. Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; iv. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan v. Memaklumkan pihak Pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	

7.14 PELUPUSAN SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN



OBJEKTIF:
Mengelakkan kebocoran maklumat daripada peralatan yang akan dilupuskan atau digunakan semula.

POLISI	PERANAN
a. Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (*overwrite*) sebelum dilupuskan atau diguna semula. b. Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh KPT dan ditempatkan di KPT. c. Peralatan ICT yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuat kuasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan KPT. d. Langkah-langkah seperti berikut hendaklah diambil:	SUB (BPM) SUB (BKP) Pegawai Aset Warga KPT Pihak Ketiga

i. Bagi peralatan ICT yang akan dilupuskan sebelum dipindah milik, data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat; ii. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; iii. Peralatan yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; iv. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; v. Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: (a) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi; (b) Mencabut, menanggalkan dan menyimpan perkakasan tambahan dalaman *Central Processing Unit* (CPU) seperti *Random Access Memory* (RAM), *hard disk*, *motherboard* dan lain-lain; (c) Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana Bahagian di KPT; (d) Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; dan (e) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan adalah di bawah tanggungjawab KPT. e. Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal; Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan; f. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer	

disalin pada media storan kedua seperti disket atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan; g. Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang berkuat kuasa; h. Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti yang ditetapkan dalam Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan i. Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori MyAsset.	

KAWALAN

KESELAMATAN TEKNOLOGI

KAWALA KESELAMATAN TEKNOLOGI TERMASUK MENENTUK TETAPAN/KONFIGURASI DALAM PERATURAN DAN PROSES DIGITAL, MENGENAL PASTI KELEMAHAN SECARA BERKALA DA MENAMBAHBAIK KESELAMATAN BAGI MENGHALANG AMCAMAN TERHADAP APLIKAIS, PANGKALAN DATA, SISTEM, INFRASTRUKTUR RANGKAIAN DAN PERALATAN KESELAMATAN SIBER.



8.1 PERANTI PENGGUNA (USER ENDPOINT DEVICES)



OBJEKTIF:
Melindungi keselamatan maklumat yang disimpan, diproses dan / atau diakses melalui peranti Pengguna.

POLISI	PERANAN
Penggunaan peranti yang disambungkan kepada rangkaian KPT/Jabatan/Agensi di bawah KPT dengan tujuan untuk menyimpan atau mengakses data rasmi kerajaan adalah tertakluk kepada keperluan dan kawalan penggunaan peranti. Peranti pengguna termasuk peranti yang disediakan oleh KPT dan peranti peribadi (BYOD) hendaklah: a. Memasang konfigurasi dan pengendalian peranti pengguna yang selamat; b. Melindungi peranti secara fizikal dengan berkunci atau setara jika peranti berada di dalam kawasan yang tidak selamat (contoh: di tempat awam, kenderaan, bilik hotel, persidangan, dan kawasan terbuka); c. Mengaktifkan mod tidur (sleep mode) atau menggunakan skrin kosong dengan kata laluan ke atas komputer; d. Peranti hendaklah dipasang dengan perisian berlesen dan perisian perlindungan yang dikemas kini; e. KPT mempunyai hak untuk mengakses data pada peranti peribadi untuk sebarang urusan keselamatan; dan f. Menyusun, menyalin, menyebarkan, melaksanakan atau cuba memperkenalkan sebarang virus atau kod komputer yang direka untuk bereplikasi sendiri, merosakkan atau sebaliknya menghalang prestasi	SUB(BPM) Pentadbir Sistem Pentadbir Rangkaian Warga KPT

	komputer atau rangkaian KPT adalah tidak dibenarkan;	

8.2 HAK AKSES ISTIMEWA



OBJEKTIF:
Memastikan hanya pengguna yang dibenarkan, komponen perisian dan perkhidmatan disediakan dengan hak akses istimewa.

POLISI	PERANAN
Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan diuruskan dengan kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas; b. Hak capaian pengguna diwujudkan, disemak, dikemas kini dan digugurkan berdasarkan peranan dan tanggungjawab pengguna; dan c. Melaksanakan pengurusan kawalan akses secara teratur dan direkodkan.	Pentadbir Sistem Pentadbir Pusat Data Pentadbir Rangkaian

8.3 SEKATAN AKSES MAKLUMAT



OBJEKTIF:
Memastikan hanya akses yang dibenarkan dan untuk menghalang capaian yang tidak dibenarkan kepada maklumat dan aset lain yang berkaitan.

POLISI	PERANAN
Capaian sistem aplikasi dan maklumat adalah terhad kepada tujuan yang dibenarkan sahaja.	Pentadbir Sistem Warga KPT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan sistem aplikasi yang dibenarkan adalah mengikut ketetapan kawalan capaian, tahap capaian dan keselamatan yang telah ditentukan; b. Memastikan jejak audit dan sistem log dilaksanakan bagi setiap aktiviti capaian sistem aplikasi dan maklumat; c. Mengehadkan capaian sistem aplikasi dan maklumat kepada tiga (3) kali percubaan. Sekiranya gagal, akaun Pengguna akan disekat; d. Mengawal capaian ke atas sistem aplikasi dan maklumat menggunakan prosedur log masuk yang selamat, kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; e. Capaian sistem aplikasi dan maklumat melalui capaian internet adalah dibenarkan dan penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja; dan f. Capaian kepada sistem aplikasi di KPT hendaklah mempunyai ciri-ciri keselamatan terkini.	

8.4 AKSES KEPADA KOD SUMBER



OBJEKTIF:
Mengelakkan fungsi yang tidak dibenarkan, perubahan yang tidak disengajakan atau berniat jahat bagi mengekalkan kerahsiaan harta intelek.

POLISI	PERANAN
Kawalan kod sumber dan dokumentasi sistem aplikasi hendaklah dilaksanakan ke atas sistem yang dibangunkan secara *outsource* dan *in-house.* Ini bagi memastikan kesinambungan sistem aplikasi itu dapat berjalan dengan	Pentadbir Sistem Pemilik Sistem

lancar sama ada selepas penyerahan sistem kepada Pemilik Sistem aplikasi atau pertukaran pegawai. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua kod sumber, dokumentasi konfigurasi dan sokongan sistem aplikasi diletakkan secara berpusat, dikawal dan direkodkan berpandukan pada garis panduan yang sedang berkuat kuasa; b. Memastikan kod sumber sistem aplikasi dan dokumentasi menjadi hak milik Kerajaan; c. Proses pengemaskinian fail sistem aplikasi hanya boleh dilakukan oleh Pentadbir Sistem ICT dan mengikut prosedur yang telah ditetapkan; d. Sebarang pindaan ke atas fail atau kod sumber sistem aplikasi perlu diuji dan disahkan sebelum penggunaan; e. Mengawal capaian ke atas kod sumber sistem aplikasi bagi mengelakkan pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan f. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	

8.5 PENGESAHAN SELAMAT



OBJEKTIF:
Memastikan pengguna atau entiti disahkan dengan selamat apabila mengakses sistem ICT, aplikasi dan perkhidmatan rangkaian.

POLISI	PERANAN
Enkripsi/penyulitan digunakan untuk melindungi kerahsiaan, integriti dan kesahihan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pentadbir Sistem Pentadbir Pusat Data Pentadbir Rangkaian

a. Teknik pengesahan yang sesuai hendaklah dipilih untuk mengesahkan identiti pengguna, perisian, mesej dan entiti lain; b. Kekuatan pengesahan harus bersesuaian dengan klasifikasi maklumat yang diakses; kaedah pengesahan termasuk penggunaan kata laluan, sijil digital, kad pintar, token atau biometrik; dan c. Prosedur untuk log masuk ke dalam sistem atau aplikasi hendaklah direka bentuk untuk meminimumkan risiko akses tidak dibenarkan.	

8.6 PENGURUSAN KAPASITI



OBJEKTIF:
Memastikan kapasiti yang diperlukan oleh fasiliti pemprosesan maklumat (ICT), sumber manusia, pejabat dan kemudahan lain.

POLISI	PERANAN
Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Kapasiti sesuatu komponen atau sistem aplikasi hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan, kegunaan dan operasi sistem aplikasi pada masa akan datang; b. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang;	ICTSO Pentadbir Sistem Pentadbir Pusat Data

c. *System Tuning* dan pemantauan sistem hendaklah diterapkan untuk memastikan ketersediaan dan kecekapan sistem; dan d. Melakukan ujian tekanan sistem dan perkhidmatan untuk mengesahkan bahawa kapasiti sistem yang mencukupi tersedia untuk memenuhi keperluan prestasi waktu puncak.	

8.7 KAWALAN DARIPADA PERISIAN HASAD (MALWARE)

OBJEKTIF:

Memastikan maklumat dan aset lain yang berkaitan dilindungi daripada perisian hasad.

POLISI	PERANAN
Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada serangan *malware* hendaklah dilaksanakan dan digabungkan dengan kesedaran Pengguna terhadap serangan tersebut. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, IDS dan IPS serta memastikan prosedur penggunaan yang betul dan selamat dipatuhi; b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c. Mengimbas peralatan ICT dengan antivirus sebelum digunakan; d. Mengemas kini antivirus dengan paten antivirus yang terkini; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;	SUB(BPM) Pentadbir Sistem Pentadbir Pusat Data Pentadbir Rangkaian Warga KPT

f. Melaksanakan program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan dalam kontrak pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus; i. Penggunaan *Mobile Code* hendaklah daripada sumber yang dipercayai dan daripada perisian yang telah mendapat jaminan kualiti sahaja; dan j. Memuat turun atau memasang perisian daripada mana-mana sistem lain di luar KPT adalah tidak dibenarkan tanpa kelulusan terlebih dahulu.	

8.8 PENGURUSAN KERENTANAN TEKNIKAL



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

POLISI	PERANAN
Kawalan daripada ancaman teknikal ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan maklumat ancaman diperoleh daripada sumber yang sahih; b. Menilai tahap kerentanan bagi mengenal pasti tahap risiko yang mungkin berlaku; dan	Pentadbir Pusat Data, Pentadbir Rangkaian

c. Mengambil dan merekodkan langkah-langkah kawalan untuk mengatasi risiko berkaitan.	

8.9 PENGURUSAN KONFIGURASI

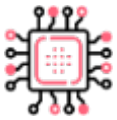


OBJEKTIF:
Memastikan perkakasan, perisian dan perkhidmatan rangkaian berfungsi dengan betul mengikut tetapan keselamatan yang diperlukan, dan konfigurasi tidak diubah oleh perubahan yang tidak dibenarkan.

POLISI	PERANAN
Pengurusan konfigurasi adalah untuk memastikan konfigurasi semua aset ICT dan sistem-sistem termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian operasi terkawal dan didokumenkan. Perkara yang perlu dipatuhi dalam pengurusan konfigurasi adalah seperti berikut: a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada Pemilik Sistem dan/atau PICT dan/atau Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana perkakasan ICT hendaklah dikendalikan oleh Pentadbir Peralatan ICT yang mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c. Semua aktiviti pengubahsuaian konfigurasi perkakasan/perisian ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkodkan dan dikawal bagi mengelakkan	Pentadbir Sistem Pemilik Sistem

berlakunya ralat sama ada secara sengaja ataupun tidak.	

8.10 PEMADAMAN MAKLUMAT



OBJEKTIF:
Maklumat yang tersimpan dalam sistem, peranti, atau media storan hendaklah dipadam apabila tiada keperluan penggunaan bagi mengelakkan pendedahan maklumat sensitif dan mematuhi keperluan undang-undang, peraturan dan kontrak.

POLISI	PERANAN
Berikut merupakan perkara yang perlu dipatuhi semasa proses penghapusan maklumat: a. Semua maklumat dalam media storan yang hendak dilupuskan mestilah dihapuskan terlebih dahulu. Proses pelupusan hendaklah dilakukan dengan teratur dan selamat mengikut tatacara atau pekeliling yang sedang berkuat kuasa; b. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan c. Bukti pemadaman maklumat hendaklah direkodkan.	SUB (BPM) Pentadbir Pusat Data Pentadbir Sistem Pentadbir e-mel UKTN

8.11 PENYEMBUNYIAN DATA (*DATA MASKING*)



OBJEKTIF:
Mengehadkan pendedahan data sensitif, termasuk PII bagi mematuhi keperluan undang-undang, berkanun, peraturan dan kontrak.

POLISI	PERANAN
Kawalan ini bertujuan untuk melindungi data sensitif atau data peribadi daripada kebocoran dengan mengaburkan	SUB(BPM) Pentadbir Sistem

atau menukar data asli kepada data yang sukar dibaca atau dikenal pasti. Berikut merupakan perkara yang perlu dipertimbangkan apabila melaksanakan *data masking*. a. Mengklasifikasikan data mengikut tahap keselamatan seperti yang ditetapkan dalam Arahan Keselamatan Kerajaan yang sedang berkuat kuasa; b. Maklumat terperingkat hanya boleh dilakukan penduaan atau penyalinan pada media storan oleh Pengguna yang dibenarkan sahaja; c. Menggunakan teknologi enkripsi dan kaedah keselamatan lain yang bersesuaian ke atas maklumat terperingkat yang disediakan dan dihantar secara elektronik; d. Memastikan data yang tidak lagi diperlukan selepas proses *masking* dipadam mengikut prosedur pelupusan semasa; dan e. Pemantauan dan penilaian berkala terhadap *data masking* hendaklah dilaksanakan untuk mengenal pasti kelemahan dan penambahbaikan.	Pentadbir Pusat Data

8.12 PENCEGAHAN KEBOCORAN DATA (*DATA LEAK PREVENTION*)



OBJEKTIF:
Mengesan dan mencegah pendedahan dan pengekstrakan maklumat yang tidak dibenarkan oleh individu atau sistem.

POLISI	PERANAN
Kawalan ini bertujuan untuk melindungi data daripada akses yang tidak sah. Ini bertujuan untuk menghalang sebarang pendedahan atau aktiviti mengekstrak data tanpa kebenaran sama ada dilakukan oleh individu atau sistem.	SUB (BPM) Pentadbir Sistem Pemilik Sistem

Berikut merupakan langkah-langkah yang perlu dilaksanakan bagi mencegah kebocoran data: a. Mengenal pasti dan mengklasifikasikan maklumat untuk melindunginya daripada kebocoran (contohnya, maklumat peribadi, model, harga, dan reka bentuk produk); b. Memantau saluran kebocoran data (contohnya, e-mel, pemindahan fail, peranti mudah alih, dan peranti penyimpanan mudah alih); c. Mengambil tindakan untuk mencegah kebocoran maklumat (contohnya, melaksanakan kuarantin e-mel yang mengandungi maklumat yang sensitif); dan d. Log daripada penyelesaian Pencegahan Ketirisan Data (DLP) hendaklah diintegrasikan dengan Sistem Maklumat Keselamatan dan Pengurusan Peristiwa (SIEM) bagi tujuan pemantauan berpusat, korelasi peristiwa untuk mengesan corak mencurigakan, dan peningkatan keupayaan tindak balas insiden secara automatik.	

8.13 SANDARAN MAKLUMAT (BACKUP)



OBJEKTIF:
Membolehkan pemulihan daripada kehilangan data atau sistem ICT.

POLISI	PERANAN
Salinan sandaran (*backup*) maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran (*backup*) yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran (*backup*) hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran (*backup*) hendaklah direkodkan dan disimpan di lokasi luar premis.	Pentadbir Sistem Pentadbir Pusat Data Pemilik Sistem

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Melaksanakan sandaran (*backup*) keselamatan ke atas semua perisian aplikasi dan sistem aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Melaksanakan sandaran (*backup*) ke atas semua data dan maklumat mengikut keperluan. Kekerapan sandaran (*backup*) bergantung pada tahap kritikal maklumat dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi; c. Sandaran (*backup*) hendaklah dilakukan di dalam media yang bersesuaian; d. Menguji secara berkala prosedur dan media sandaran (*backup*) dan *restore* bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila perlu digunakan; e. Membangunkan dan melaksanakan pengurusan generasi sandaran (*backup*) berdasarkan pelan pengurusan risiko bagi setiap aset ICT; f. Merekodkan dan menyimpan salinan sandaran (*backup*) di lokasi yang berlainan dan selamat; dan g. Sandaran (*backup*) hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan atau tahunan.	

8.14 PERTINDIHAN KEMUDAHAN PEMPROSESAN MAKLUMAT



OBJEKTIF:
Memastikan kemudahan pemprosesan maklumat terus beroperasi tanpa gangguan.

POLISI	PERANAN
Keperluan redundansi/replikasi kemudahan pemprosesan maklumat hendaklah dikenal pasti bagi memastikan ketersediaan perkhidmatan dan sistem ICT. Perkara-perkara berikut hendaklah dipertimbangkan (tetapi tidak terhad kepada): a. Membangunkan kontrak dengan dua atau lebih pembekal rangkaian dan kemudahan pemprosesan maklumat kritikal seperti pembekal perkhidmatan internet; b. Menggunakan rangkaian redundansi; c. Menggunakan bekalan kuasa atau sumber redundansi secara fizikal; d. Menggunakan pelbagai komponen perisian selari, dengan pengimbangan beban (*load balancing*) automatik; e. Mempunyai komponen pendua dalam sistem (contoh: CPU, cakera keras, memori) atau dalam rangkaian (suis, *firewall*); f. Mempunyai komponen pendua dalam sistem (contoh: CPU, cakera keras, memori) atau dalam rangkaian (contoh: *firewall*, penghala, suis); dan g. Kemudahan pemprosesan maklumat (ICT) (termasuk infrastruktur, sistem, aplikasi, pangkalan data dan storan) hendaklah diuji untuk memastikan *failover* dari satu komponen ke komponen lain berfungsi dengan baik.	SUB (BPM) Pentadbir Sistem Pemilik Sistem

8.15 PENGELOGAN



OBJEKTIF:
Merekodkan insiden, menjana bukti, memastikan integriti maklumat log, mencegah capaian yang tidak dibenarkan, mengenal pasti insiden keselamatan maklumat yang boleh menyokong penyiasatan.

POLISI	PERANAN
8.15.1 *Sistem Log*	
a. Fail log hendaklah disimpan untuk tempoh sekurang-kurangnya tiga (3) bulan. Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti berikut: I. Fail log sistem pengoperasian; II. Fail log servis (web, e-mel); III. Fail log aplikasi (jejak audit); dan IV. Fail log rangkaian (*switch, firewall*, IPS). b. Perkara-perkara berikut hendaklah dilaksanakan: I. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; II. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan III. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada ICTSO dan CDO.	SUB (BPM) Pentadbir sistem Pemilik Sistem
8.15.2 Pemantauan Log	
Perkara-perkara berikut hendaklah dilaksanakan: a. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;	SUB (BPM) Pentadbir sistem Pemilik Sistem

b. Prosedur untuk memantau penggunaan kemudahan memproses maklumat hendaklah dibangunkan dan hasilnya perlu dipantau secara berkala; c. Kemudahan merekodkan dan maklumat log mestilah dilindungi daripada diubah suai dan sebarang capaian yang tidak dibenarkan; d. Aktiviti pentadbiran dan operator/pembekal sistem hendaklah direkodkan; e. Kesalahan, kesilapan dan/atau penyalahgunaan mesti direkodkan, dianalisis dan diambil tindakan sewajarnya; dan f. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam KPT atau domain keselamatan mesti diselaraskan dengan satu sumber waktu yang dipersetujui.	

8.16 PEMANTAUAN AKTIVITI ICT



OBJEKTIF:
Merekodkan insiden, menjana bukti, memastikan integriti maklumat log, mencegah capaian yang tidak dibenarkan, mengenal pasti insiden keselamatan maklumat yang boleh menyokong penyiasatan.

POLISI	PERANAN
Perkara-perkara berikut hendaklah dipertimbangkan dalam melaksanakan aktiviti pemantauan: a. Rangkaian keluar dan masuk, trafik sistem dan aplikasi; b. Akses kepada sistem, pelayan, peralatan rangkaian, sistem pemantauan, aplikasi kritikal, dll.; c. Fail konfigurasi sistem atau rangkaian yang kritikal;	SUB (BPM)

d. Log daripada alatan keselamatan (contoh:antivirus, IDS, IPS); e. Log kejadian yang berkaitan dengan sistem dan aktiviti rangkaian; f. Menyemak bahawa kod yang sedang dilaksanakan dibenarkan untuk dijalankan dan tidak diusik (*tampered*); dan g. Penggunaan sumber dan prestasinya (contoh: CPU, cakera keras, memori).	

8.17 PENYERAGAMAN JAM



OBJEKTIF:
Membolehkan korelasi dan analisis insiden berkaitan keselamatan dan data lain yang direkodkan bagi menyokong penyiasatan terhadap insiden keselamatan maklumat.

POLISI	PERANAN
a. Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal; dan b. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam KPT atau domain keselamatan perlu diseragamkan dari satu sumber waktu yang selaras dengan *Malaysia Standard Time* (MST).	SUB (BPM)

8.18 PENGGUNAAN PROGRAM UTILITI



OBJEKTIF :
Memastikan penggunaan program utiliti tidak membahayakan rangkaian dan keselamatan maklumat.

POLISI	PERANAN

a. Program utiliti ialah sebarang perisian yang direka untuk menganalisis atau menyelenggara sistem atau rangkaian komputer. b. Mengawal Penggunaan program utiliti kepada Pengguna atau penyelenggara ICT yang dibenarkan sahaja.	SUB (BPM)

8.19 PEMASANGAN PERISIAN PADA SISTEM OPERASI



OBJEKTIF: Memastikan integriti sistem operasi dan mencegah eksploitasi kelemahan teknikal.

POLISI	PERANAN
Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa meluluskan adalah seperti berikut: a. Pemasangan dan pengemaskinian perisian sistem pengoperasian, aplikasi dan *program libraries* hanya boleh dilakukan setelah mendapat kelulusan pemilik sistem; b. Memastikan penggunaan perisian mempunyai lesen sah; c. Strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian; d. Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperakukan berjaya; dan e. Setiap konfigurasi sistem dan perisian perlu dikawal dan log audit perlu diaktifkan.	Pentadbir Sistem Pentadbir Pusat Data

8.20 KESELAMATAN RANGKAIAN



OBJEKTIF:
Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.

POLISI	PERANAN
Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara yang perlu dipatuhi adalah seperti berikut: a. Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas daripada risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja; d. Sebarang penyambungan rangkaian yang bukan di bawah kawalan BPM, KPT adalah tidak dibenarkan; e. Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di KPT sahaja dan penggunaan MODEM adalah dilarang sama sekali; f. Kemudahan bagi *wireless* LAN hendaklah dipantau dan dikawal penggunaannya; dan g. Memastikan Rajah keseluruhan rangkaian (fizikal dan logikal) KPT hendaklah terkini dan merangkumi kawalan keselamatan termaju yang merangkumi: *Firewall* generasi baharu (NGFW), Sistem Pengesanan dan Pencegahan Pencerobohan (IDPS), Sistem Pengurusan Maklumat dan Peristiwa Keselamatan (SIEM), serta pemakaian Seni Bina *Zero Trust* (ZTA) yang memastikan setiap pengguna, peranti dan aplikasi sentiasa disahkan sebelum diberi akses.	SUB(BPM) ICTSO Pentadbir Rangkaian

h. Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan.	

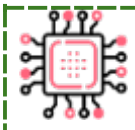
8.21 KESELAMATAN PERKHIDMATAN



OBJEKTIF:
Memastikan keselamatan dalam penggunaan perkhidmatan rangkaian.

POLISI	PERANAN
Pengurusan bagi semua perkhidmatan rangkaian (*in-house* atau *outsource*) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan dalam perjanjian perkhidmatan rangkaian dengan cara: a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pihak ketiga; b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit; dan c. Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Pentadbir Rangkaian

8.22 PENGASINGAN RANGKAIAN



OBJEKTIF:
Mengasingkan rangkaian dalaman mengikut sempadan keselamatan dan mengawal trafik antara rangkaian tersebut berdasarkan keperluan perkhidmatan.

POLISI	PERANAN
Perkara-perkara berikut hendaklah dilaksanakan: a. Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan Pengguna dan sistem maklumat mengikut segmen rangkaian KPT; b. Pengasingan merangkumi tindakan memisahkan rangkaian antara kumpulan operasi (*production*) dan pembangunan/pengujian (*development/testing*); dan c. Perkakasan berkaitan yang digunakan bagi tugas membangunkan, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*.	Pentadbir Rangkaian

8.23 PENAPISAN LAMAN (WEB)



OBJEKTIF:
Melindungi sistem daripada dikompromi oleh perisian terlarang dan untuk menghalang akses kepada sumber web yang tidak dibenarkan.

POLISI	PERANAN
Capaian Internet bagi urusan rasmi membolehkan Pengguna berhubung dan mencapai maklumat dalam persekitaran yang selamat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pemantauan secara berterusan hendaklah dilakukan bagi memastikan penggunaannya hanya untuk capaian yang dibenarkan sahaja; b. Penguatkuasaan *Content Filtering* hendaklah dilaksanakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;	Pentadbir Rangkaian

c. Pengawalan penggunaan *bandwidth* hendaklah dilaksanakan bagi penggunaan *bandwidth* yang maksimum dan lebih berkesan; d. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja; e. Pengguna hanya dibenarkan memuat turun perisian yang sah dan berdaftar; f. Perolehan/pembelian dan penggunaan *broadband* bergantung pada justifikasi atau keperluan dan perlu mendapat kelulusan ; dan g. Penggunaan kemudahan internet peribadi di pejabat seperti modem, *hotspot* dan sebagainya untuk tujuan sambungan ke internet perlu mendapat kelulusan jika melibatkan sambungan ke rangkaian KPT.	

8.24 PENGGUNAAN KRIPTOGRAFI



OBJEKTIF:
Memastikan Penggunaan kriptografi yang betul dan berkesan untuk melindungi kerahsiaan dan integriti maklumat mengikut keperluan keselamatan perkhidmatan dan maklumat, dengan mengambil kira keperluan undang-undang, berkanun, peraturan dan kontrak yang berkaitan dengan kriptografi.

POLISI	PERANAN
Perkara-perkara berikut hendaklah dilaksanakan: a. Peraturan untuk Penggunaan kriptografi yang berkesan termasuk pengurusan kunci kriptografi, hendaklah ditakrifkan dan dilaksanakan; b. Menyediakan kaedah HTTPS bagi pembangunan aplikasi laman yang akan digunakan/diakses oleh orang awam;	SUB (BPM) Pentadbir Sistem Warga KPT

c. Memastikan Sijil SSL dipasang ke atas aplikasi yang telah ditentukan oleh KPT; d. Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat Rahsia dan Rahsia Besar pada setiap masa; dan e. Menggunakan tandatangan digital/ PKI bagi menguruskan transaksi maklumat rahsia rasmi secara elektronik. f. Menyediakan inventori data kriptografi dan melaksanakan perancangan Post-Quantum Cryptography (PQC) bagi sistem yang dikategorikan sebagai NCII.	

8.25 KITARAN HAYAT PEMBANGUNAN SISTEM/APLIKASI YANG SELAMAT



OBJEKTIF :
Memastikan keselamatan maklumat direka dan dilaksanakan dalam kitaran hayat Pembangunan perisian dan sistem yang selamat.

POLISI	PERANAN
Pembangunan perisian dan sistem yang selamat hendaklah dilaksanakan seperti berikut: a. Pembangunan selamat ialah keperluan untuk membina perkhidmatan, seni bina, perisian dan sistem yang selamat (keselamatan dalam kitaran hayat pembangunan perisian); b. Perubahan kepada sistem dalam kitaran hayat Pembangunan mesti dikawal dengan menggunakan prosedur kawalan perubahan formal; c. Apabila platform pengendalian ditukar, aplikasi kritikal perkhidmatan mesti disemak dan diuji untuk memastikan tiada kesan buruk terhadap operasi atau keselamatan organisasi;	Pentadbir Sistem Pemilik Sistem

d. Pengubahsuaian pada pakej perisian dan semua perubahan mesti dikawal dengan ketat; dan e. Pembangunan aplikasi mudah alih yang melibatkan integrasi dengan sistem induk hendaklah menggunakan *Application Programming Interface* (API) atau lain-lain kaedah yang bersesuaian yang tidak memberi risiko ancaman keselamatan.	

8.26 KEPERLUAN KESELAMATAN APLIKASI



OBJEKTIF:
Memastikan semua keperluan keselamatan maklumat dikenal pasti dan ditangani semasa membangunkan atau memperoleh aplikasi.

POLISI	PERANAN
Keperluan keselamatan maklumat perlu dikenal pasti, ditentukan, dan diluluskan sebelum fasa pembangunan atau perolehan dimulakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Melaksanakan pengelasan data, pengasingan akses berdasarkan peranan dan tanggungjawab; b. Melaksanakan perlindungan ke atas data yang sedang diproses, data dalam transit dan data dalam simpanan berdasarkan pekeliling dan undang-undang semasa yang sedang berkuat kuasa; c. Melaksanakan kawalan bagi semua proses input, proses automasi, dan proses output sesuatu aplikasi; d. Melaksanakan kawalan keselamatan berdasarkan keperluan bisnes dan keselamatan data; dan e. Melaksanakan pengendalian mesej ralat. f. Sistem atau aplikasi yang menguruskan pembayaran dalam talian hendaklah mematuhi Piawaian	SUB (BPM) Pentadbir Sistem Pemilik Sistem

Keselamatan Data Industri Kad Pembayaran (PCI-DSS) dengan menggunakan gerbang pembayaran selamat yang mempunyai fungsi penyulitan (enkripsi) dan tokenisasi, di samping penggunaan penyelesaian anti-DDoS.	

8.27 SENIBINA SISTEM SELAMAT DAN PRINSIP KEJURUTERAAN



OBJEKTIF:
Memastikan sistem maklumat direka bentuk, dilaksanakan dan dikendalikan dengan selamat dalam kitaran hayat pembangunan.

POLISI	PERANAN
Prinsip kejuruteraan dan arkitektur sistem yang selamat merujuk kepada penyediaan dan penggunaan amalan terbaik dalam proses pembangunan dan reka bentuk sistem aplikasi yang menitikberatkan aspek keselamatan dan perlindungan maklumat. a. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Aspek keselamatan perlu diterapkan dalam semua peringkat arkitektur (bisnes, data, aplikasi dan teknologi); ii. Teknologi baharu perlu dianalisis bagi mengenal pasti risiko keselamatan dan reka bentuk arkitektur perlu dikaji semula berdasarkan corak serangan siber yang diketahui; iii. Melaksanakan analisis terhadap ancaman yang dikenal pasti, keupayaan dan pelaksanaan kawalan keselamatan bagi menangani ancaman; dan iv. Melaksanakan pengukuhan keselamatan arkitektur sistem aplikasi berdasarkan kawalan keselamatan yang dikenal pasti. b. Prinsip kejuruteraan sistem yang selamat termasuk, tetapi tidak terhad kepada: i. Menyediakan panduan mengenai kaedah pengesahan pengguna;	SUB (BPM) Pemilik sistem Pentadbir sistem

ii. Menyediakan panduan kawalan sesi selamat; iii. Menyediakan panduan mengenai prosedur sanitasi dan pengesahan data; iv. Menganalisis secara menyeluruh tentang semua langkah keselamatan yang diperlukan untuk melindungi aset dan sistem maklumat daripada ancaman yang diketahui; v. Menganalisis secara menyeluruh tentang keupayaan Langkah keselamatan untuk mengenal pasti, menghapuskan dan bertindak balas terhadap ancaman keselamatan; vi. Menganalisis langkah keselamatan yang digunakan untuk aktiviti perkhidmatan tertentu seperti penyulitan maklumat; vii. Menyediakan Langkah keselamatan bagi pelaksanaan penyepaduan kawalan keselamatan khusus bagi infrastruktur teknikal; dan viii. Menyediakan kawalan keselamatan yang berbeza, yang boleh berfungsi dan beroperasi sebagai set kawalan gabungan.	

8.28 PENGEKODAN SELAMAT



OBJEKTIF:
Memastikan perisian dibangunkan dengan selamat dan mengurangkan potensi kelemahan keselamatan maklumat dalam perisian.

POLISI	PERANAN
Prinsip pengaturcaraan selamat (*secure coding*) hendaklah dilaksanakan dalam pengurusan sistem aplikasi. Ancaman terkini dan teknologi semasa perlulah diambil kira untuk memastikan prinsip pengaturcaraan selamat dapat dilaksanakan dengan berkesan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Menggunakan teknik pengaturcaraan yang berstruktur dan selamat; b. Perancangan dan pemilihan teknologi persekitaran pengurusan aplikasi hendaklah mengambil kira	SUB (BPM) Pentadbir sistem Pemilik Sistem

ancaman dan teknologi semasa serta sokongan terhadap teknologi yang digunakan; c. Penggunaan aplikasi sokongan atau kod atur cara pihak ketiga perlu sentiasa dipantau dan dikemas kini ke versi terkini; dan d. Pengemaskinian ini hendaklah mengambil kira kesesuaian sistem dan impak terhadap pelaksanaan aplikasi berkenaan.	

8.29 UJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN



OBJEKTIF:
Mengesahkan bahawa keperluan keselamatan maklumat dipenuhi apabila aplikasi atau kod digunakan dalam persekitaran pengeluaran (*production*).

POLISI	PERANAN
Ujian dalam pembangunan dan penerimaan mestilah mengikut perkara berikut: a. Ujian kefungsian keselamatan mesti dijalankan semasa pembangunan; b. Ujian Prestasi (*Performance Test*) hendaklah dilaksanakan dan direkodkan sebelum sesuatu sistem dibenarkan beroperasi (*go-live*) atau mengikut keperluan bagi mengesahkan daya tahan dan kestabilan prestasi sistem tersebut. c. Persekitaran ujian dan operasi mesti diasingkan untuk mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi; dan d. Kriteria penerimaan untuk sistem maklumat baharu, naik taraf, dan versi baharu mesti diwujudkan dan ujian yang sesuai bagi sistem hendaklah dijalankan sebelum penerimaan.	Pemilik sistem Pentadbir Sistem

8.30 PEMBANGUNAN OLEH SUMBER LUAR (*OUTSOURCE*)



OBJEKTIF:
Memastikan Langkah keselamatan maklumat yang diperlukan oleh organisasi dilaksanakan dalam pembangunan sistem oleh sumber luar.

POLISI	PERANAN
a. Aktiviti pembangunan sistem oleh sumber luar hendaklah diselia dan dipantau termasuk: i. Pengurusan lesen sistem, pemilikan kod dan hak intelek; ii. Jaminan kualiti; iii. Pengurusan hak akses; dan iv. Ujian keselamatan. b. Pembangunan perisian aplikasi secara *outsource* hendaklah mematuhi perkara-perkara berikut: i. Setiap projek perlu dipantau oleh pemilik sistem; ii. Kontrak Pembekalan hendaklah memasukkan klausa kod sumber menjadi hak milik KPT; iii. Kod sumber yang diserahkan kepada KPT mesti bebas daripada sebarang ralat dan kerentanan; iv. Mengutamakan kepakaran teknologi tempatan; v. Pembangunan aplikasi hendaklah dijalankan dalam persekitaran pengkomputeran KPT; vi. Penggunaan *data masking* semasa pengujian; vii. Data ujian hendaklah dilupuskan secara kekal *(secured delete)* selepas projek disiapkan atau tamat kontrak; dan viii. Aktiviti sandaran *(backup)* hendaklah berjaya dilakukan sebelum projek tamat. c. Data yang terlibat dalam sistem aplikasi perlu disahkan bagi memelihara integriti data. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Data *input* bagi sistem aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan tepat;	Pemilik Sistem Pentadbir Sistem Pihak Ketiga

ii. Data *output* daripada sistem aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat; iii. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; iv. Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; v. Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian; vi. Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan vii. Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar.	

8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PENGELUARAN (PRODUCTION)



OBJEKTIF:
Melindungi persekitaran pengeluaran dan data daripada kompromi oleh aktiviti Pembangunan dan pengujian.

POLISI	PERANAN
Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan risiko pengubahsuaian tanpa kebenaran, perubahan yang tidak disengajakan atau penyalahgunaan aset. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Skop tugas dan tanggungjawab termasuk mewujudkan, memadam, mengemas kini, mengubah dan mengesahkan perlu diasingkan bagi mengurangkan risiko berlakunya penyalahgunaan, akses atau pengubahsuaian yang tidak dibenarkan ke	Pentadbir Sistem Pentadbir Pusat Data Pentadbir Rangkaian

atas aset ICT daripada ralat, kebocoran maklumat terperingkat atau dimanipulasi; b. Aset ICT yang digunakan bagi tugas membangunkan, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan daripada aset ICT yang digunakan sebagai persekitaran sebenar (*production*). Pengasingan juga merangkumi tindakan memisahkan antara kumpulan pembangun sistem dan pelaksana operasi; dan c. Pengasingan tugas bagi tugasan yang bersifat kritikal tidak boleh dilaksanakan oleh seorang individu sahaja atas kuasa tunggalnya dan hendaklah dikendalikan dalam tadbir urus yang bersesuaian.	

8.32 PENGURUSAN PERUBAHAN

OBJEKTIF:
Memelihara keselamatan maklumat semasa melaksanakan perubahan

POLISI	PERANAN
Perubahan pada sistem aplikasi dalam kitaran hayat pembangunan hendaklah dikawal dengan menggunakan Prosedur Kawalan Perubahan Sistem yang telah ditetapkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perubahan sistem aplikasi hendaklah dirancang dan dinilai berdasarkan impak yang mungkin berlaku serta mengambil kira semua kebergantungan pada sistem berkenaan. Perubahan tersebut hendaklah dikaji, diuji, direkodkan dan disahkan sebelum diguna pakai; b. PICT dan Pentadbir Sistem ICT perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal;	Pentadbir Sistem Pemilik Sistem Pentadbir Pusat Data

c. Akses kepada kod sumber sistem aplikasi perlu dihadkan kepada Pengguna yang dibenarkan sahaja; dan d. Sebarang kemungkinan kebocoran maklumat hendaklah dihalang.	

8.33 MAKLUMAT UJIAN



OBJEKTIF:
Memastikan keperluan ujian dan perlindungan maklumat operasi yang digunakan untuk ujian.

POLISI	PERANAN
Keperluan keselamatan maklumat perlu dikenal pasti, ditentukan, dan diluluskan sebelum fasa pembangunan atau perolehan dimulakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Melaksanakan pengelasan data, pengasingan akses berdasarkan peranan dan tanggungjawab; b. Melaksanakan perlindungan ke atas data yang sedang diproses, data dalam transit dan data dalam simpanan berdasarkan pekeliling dan undang-undang semasa yang sedang berkuat kuasa; c. Melaksanakan kawalan bagi semua proses input, proses automasi, dan proses output sesuatu aplikasi; d. Melaksanakan kawalan keselamatan berdasarkan keperluan bisnes dan keselamatan data; dan e. Melaksanakan pengendalian mesej ralat.	Pemilik Sistem Pentadbir Sistem Pihak Ketiga

8.34 PERLINDUNGAN SISTEM MAKLUMAT ICT SEMASA PENGUJIAN/PENGAUDITAN



OBJEKTIF:
Meminimumkan kesan pengauditan dan aktiviti pengujian ke atas sistem maklumat ICT dan proses perkhidmatan yang lain.

POLISI	PERANAN
Perlindungan sistem maklumat semasa pengujian/ pengauditan mestilah meminimumkan ancaman dan memaksimumkan keberkesanan aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Jejak audit (log) hendaklah diaktifkan untuk merekodkan perubahan kepada maklumat sensitif dalam semua sistem ICT, termasuk menjejaki setiap penambahan, pengubahsuaian dan pemadaman maklumat; b. Jejak audit (log) peristiwa keselamatan maklumat mesti disemak secara berkala dengan pengetahuan/ Kemahiran yang sesuai. Kekerapan semakan mesti bergantung pada risiko yang terlibat; dan c. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas operasi aset ICT perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.	ICTSO SUB BPM Pentadbir Sistem Pentadbir Pusat Data Pentadbir Rangkaian

JADUAL MAPPING ANNEX 27001:2022 KEPADA BIDANG PKS KPT VERSI 3.0

BIL	ISMS 27001:2022		PKS KPT v3.0	
	ANNEX	KAWALAN	KAWALAN	BIDANG
1.	5.1	*Policies for information security*	5.1	Polisi Keselamatan Siber
2.	5.2	*Information security roles and responsibilities*	5.2	Peranan Dan Tanggungjawab Keselamatan Maklumat
3.	5.3	*Segregation of duties*	5.3	Pengasingan Tugas
4.	5.4	*Management responsibilities*	5.4	Tanggungjawab Pengurusan
5.	5.5	*Contact with authorities*	5.5	Hubungan Dengan Pihak Berkuasa
6.	5.6	*Contact with special interest groups*	5.6	Hubungan Dengan Pihak Berkepentingan Yang Khusus
7.	5.7	*Threat Intelligence* - **NEW**	5.7	Kecerdasan Ancaman (*Threat Intelligence*)
8.	5.8	*Information security in project management*	5.8	Keselamatan Maklumat Dalam Pengurusan Projek
9.	5.9	*Inventory of information and other associated assets*	5.9	Inventori Maklumat Dan Aset Lain Yang Berkaitan
10.	5.10	*Acceptable use of information and other associated assets*	5.10	Penerimaan Dan Penggunaan Maklumat Dan Aset ICT
11.	5.11	*Return of assets*	5.11	Pemulangan Aset
12.	5.12	*Classification of information*	5.12	Klasifikasi Maklumat
13.	5.13	*Labelling of information*	5.13	Pelabelan Maklumat
14.	5.14	*Information transfer*	5.14	Pemindahan Maklumat
15.	5.15	*Access control*	5.15	Kawalan Akses
16.	5.16	*Identity management*	5.16	Pengurusan Identiti
17.	5.17	*Authentication information*	5.17	Pengesahan Identiti

BIL	ISMS 27001:2022		PKS KPT v3.0	
	ANNEX	KAWALAN	KAWALAN	BIDANG
18.	5.18	*Access rights*	5.18	Hak Akses
19.	5.19	*Information security in supplier relationships*	5.19	Keselamatan Maklumat Dan Pengurusan Pembekal
20.	5.20	*Addressing information security within supplier agreement*	5.20	Menangani Keselamatan Maklumat Di Dalam Perjanjian Pembekal
21.	5.21	*Managing information security in the information and communication technology (ICT) supply chain*	5.21	Menguruskan Keselamatan Maklumat Dalam Rantaian Bekalan ICT
22.	5.22	*Monitoring, review and change management of supplier services*	5.22	Memantau, Mengkaji Dan Pengurusan Perubahan Perkhidmatan Pembekal
23.	5.23	*Information security for use of cloud services* - **NEW**	5.23	Keselamatan Maklumat Untuk Penggunaan Perkhidmatan Awan
24.	5.24	*Information security incident management planning and preparation*	5.24	Pelan Dan Penyediaan Pengurusan Insiden Keselamatan Maklumat
25.	5.25	*Assessment and decision on information security events*	5.25	Penilaian dan Keputusan Insiden Keselamatan Maklumat
26.	5.26	*Response to information security incidents*	5.26	Tindak balas Terhadap Insiden Keselamatan Maklumat
27.	5.27	*Learning from information security incidents*	5.27	Pengajaran Dari Insiden Keselamatan Maklumat
28.	5.28	*Collection of evidence*	5.28	Pengumpulan Bukti
29.	5.29	*Information security during disruption*	5.29	Keselamatan Maklumat Semasa Gangguan

BIL	ISMS 27001:2022		PKS KPT v3.0	
	ANNEX	KAWALAN	KAWALAN	BIDANG
30.	5.30	*ICT readiness for business continuity* - **NEW**	5.3	Kesediaan ICT Untuk Kesinambungan Perkhidmatan
31.	5.31	*Legal, statutory, regulatory and contractual requirements*	5.31	Keperluan Undang-undang, Kanun, Peraturan Dan Kontrak
32.	5.32	*Intellectual property rights*	5.32	Hak Harta Intelek
33.	5.33	*Protection of records*	5.33	Perlindungan Rekod
34.	5.34	*Privacy and protection of personal identifiable information* (PII)	5.34	Privasi Dan Perlindungan Maklumat Pengenalan Peribadi
35.	5.35	*Independent review of information security*	5.35	Kajian Bebas Keselamatan Maklumat
36.	5.36	*Compliance with policies, rules, and standards for information security*	5.36	Pematuhan Dengan Polisi, Peraturan Dan Piawaian Untuk Keselamatan Maklumat
37.	5.37	*Documented operating procedures*	5.37	Prosedur Operasi Yang Didokumenkan
38.	6.1	*Screening*	6.1	Saringan
39.	6.2	*Terms and conditions of employment*	6.2	Terma Dan Syarikat Perkhidmatan
40.	6.3	*Information security awareness, education and training*	6.3	Kesedaran, Pendidikan Dan Latihan Keselamatan Maklumat
41.	6.4	*Disciplinary process*	6.4	Proses Tatatertib
42.	6.5	*Responsibilities after termination or change of employment*	6.5	Penamatan Atau Pertukaran Perjawatan
43.	6.6	*Confidentiality or non-disclosure agreements*	6.6	Perjanjian Kerahsiaan Atau Keterdedahan
44.	6.7	*Remote working*	6.7	Telekerja

BIL	ISMS 27001:2022		PKS KPT v3.0	
	ANNEX	KAWALAN	KAWALAN	BIDANG
45.	6.8	*Information security event reporting*	6.8	Pelaporan Insiden Keselamatan Maklumat
46.	7.1	*Physical security perimeters*	7.1	Perimeter Keselamatan Fizikal
47.	7.2	*Physical entry*	7.2	Kemasukan Fizikal
48.	7.3	*Securing offices, rooms and facilities*	7.3	Keselamatan Pejabat, Bilik Dan Kemudahan
49.	7.4	*Securing offices, rooms and facilities* - **NEW**	7.4	Pemantauan Keselamatan Fizikal
50.	7.5	*Protecting against physical and environment threats*	7.5	Perlindungan Daripada Ancaman Luar Dan Persekitaran
51.	7.6	*Working in secure areas*	7.6	Bekerja Di Kawasan Selamat
52.	7.7	*Clear desk and clear screen*	7.7	Meja Bersih Dan Skrin Kosong
53.	7.8	*Equipment sitting and protection*	7.8	Penempatan Dan Perlindungan Peralatan
54.	7.9	*Security of assets off-premises*	7.9	Perlindungan Aset Di luar Premis
55.	7.10	*Storage media*	7.10	Media Storan
56.	7.11	*Supporting Utilities*	7.11	Utiliti Sokongan
57.	7.12	*Cabling Security*	7.12	Keselamatan Kabel
58.	7.13	*Equipment Maintenance*	7.13	Penyelenggaraan Peralatan
59.	7.14	*Secure disposal or re-use of equipment*	7.14	Pelupusan Selamat Atau Penggunaan Semula Peralatan
60.	8.1	*User end point devices*	8.1	Peranti Pengguna
61.	8.2	*Privileged access rights*	8.2	Hak Akses Istimewa
62.	8.3	*Information access restriction*	8.3	Sekatan Akses Maklumat

BIL	ISMS 27001:2022		PKS KPT v3.0	
	ANNEX	KAWALAN	KAWALAN	BIDANG
63.	8.4	*Access to source code*	8.4	Akses Kepada Kod Sumber
64.	8.5	*Secure authentication*	8.5	Pengesahan Selamat
65.	8.6	*Capacity management*	8.6	Pengurusan Kapasiti
66.	8.7	*Protection against malware*	8.7	Kawalan Daripada Perisian Hasad (*Malware*)
67.	8.8	*Management of technical vulnerabilities*	8.8	Pengurusan Kerentanan Teknikal
68.	8.9	*Configuration management* – **NEW**	8.9	Pengurusan Konfigurasi
69.	8.10	*Information deletion* – **NEW**	8.10	Pemadaman Maklumat
70.	8.11	*Data masking* - **NEW**	8.11	Penyembunyian Data (*Data Masking*)
71.	8.12	*Data leakage prevention* - **NEW**	8.12	Pencegahan Kebocoran Data
72.	8.13	*Information backup*	8.13	Sandaran Maklumat (*Backup*)
73.	8.14	*Redundancy of information processing facilities*	8.14	Pertindihan Kemudahan Pemprosesan Maklumat
74.	8.15	*Logging*	8.15	Pengelogan
75.	8.16	*Monitoring activities* - **NEW**	8.16	Pemantauan Aktiviti ICT
76.	8.17	*Clock synchronization*	8.17	Penyeragaman Jam
77.	8.18	*Use of privileged utility programs*	8.18	Penggunaan Program Utiliti
78.	8.19	*Installation of software on operational systems*	8.19	Pemasangan Perisian Pada Sistem Operasi
79.	8.20	*Networks security*	8.20	Keselamatan Rangkaian
80.	8.21	*Security of network services*	8.21	Keselamatan Perkhidmatan Rangkaian

BIL	ISMS 27001:2022		PKS KPT v3.0	
	ANNEX	KAWALAN	KAWALAN	BIDANG
81.	8.22	*Segregation of networks*	8.22	Pengasingan Rangkaian
82.	8.23	*Web Filtering* - **NEW**	8.23	Penapisan Laman Web
83.	8.24	*Use of cryptography*	8.24	Penggunaan Kriptografi
84.	8.25	*Secure development life cycle*	8.25	Kitaran Hayat Pembangunan Sistem. Aplikasi Yang Selamat
85.	8.26	*Application security requirement*	8.26	Keperluan Keselamatan Aplikasi
86.	8.27	*Secure system architecture and engineering principles*	8.27	Seni bina Sistem Selamat Dan Prinsip Kejuruteraan
87.	8.28	*Secure coding* - ***NEW***	8.28	Pengekodan Selamat
88.	8.29	*Security testing in development and acceptance*	8.29	Ujian Selamat Dalam Pembangunan Dan Penerimaan
89.	8.30	*Outsourced development*	8.30	Pembangunan Oleh Sumber Luar (*Outsource*)
90.	8.31	*Separation of development, test and production environments*	8.31	Pengasingan Persekitaran Pembangunan, Pengujian Dan Pengeluaran (*Production*)
91.	8.32	*Change Management*	8.32	Pengurusan Perubahan
92.	8.33	*Test information*	8.33	Maklumat Ujian
93.	8.34	*Protection of information systems during audit testing*	8.34	Perlindungan Sistem Maklumat ICT Semasa Pengujian/ Pengauditan

Petunjuk :

Kawalan Baru

SENARAI PERUNDANGAN DAN PERATURAN YANG BERKAITAN

1. Akta Rahsia Rasmi 1972;
2. Perintah-Perintah Am;
3. Arahan Perbendaharaan
4. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama) - “Tatacara Penyediaan, Penilaian dan Penerimaan Tender”;
5. Surat Pekeliling Perbendaharaan Bil. 3/1995 - “Peraturan Perolehan Perkhidmatan Perundingan”;
6. Akta Tandatangan Digital 1997;
7. Akta Jenayah Komputer 1997;
8. Akta Hak Cipta (Pindaan) Tahun 1997;
9. Akta Komunikasi dan Multimedia 1998;
10. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”;
11. Pekeliling Am Bilangan 4 Tahun 2022 bertajuk “Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam”;
12. Surat Akujanji (Pekeliling Perkhidmatan Bilangan 17 Tahun 2001);
13. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)”;
14. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002;
15. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan”;
16. Surat Pekeliling Am Bilangan 3 Tahun 2024 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
17. Surat Pekeliling Am Bil. 4 Tahun 2006 – “Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam”;
18. Pekeliling Perbendaharaan 5 Tahun 2007 bertajuk “Tatacara Pengurusan Aset Alih Kerajaan (TPA)”;
19. Pekeliling Perkhidmatan Bil 5 2007 bertajuk “Panduan Pengurusan Pejabat” bertarikh 30 April 2007;

20. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 “Langkah-langkah mengenai Penggunaan Mel Elektronik Agensi – Agensi Kerajaan”, Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan *Government Unified Communication* (MyGovUC);
21. Arahan Teknologi Maklumat 2007;
22. Surat Arahan MAMPU.702-1/1/7 Jld. 3 (48) bertarikh 23 Mac 2009 bertajuk “Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-agensi Kerajaan”;
23. Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 bertajuk “Penggunaan Media Jaringan Sosial di Sektor Awam”;
24. Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2013 Dalam Sektor Awam;
25. Pekeliling Kemajuan Pentadbiran Awam Bilangan 3 Tahun 2015 bertajuk “Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [*Government Public Key Infrastructure* (GPKI)]” bertarikh 23 Oktober 2015;
26. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), April 2016;
27. Arahan Keselamatan (Semakan dan Pindaan 2017);
28. Pekeliling Perkhidmatan Bilangan 5 Tahun 2020. Dasar Bekerja Dari Rumah;
29. Arahan Pentadbiran Ketua Pengarah MAMPU Bilangan 4 Tahun 2020 - Polisi Keselamatan Siber MAMPU;
30. Surat edaran arahan dalaman KPT.500-7/3/1(82) bertarikh 31 Mei 2021 berkaitan Pematuhan Mesyuarat Atas Talian;
31. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2001 bertajuk “Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam” bertarikh 10 Jun 2021;
32. Pekeliling Am Bilangan 5 Tahun 2021 Tapisan Keselamatan Semula Kepada Pegawai Awam Melalui Sistem e-Vetting.
33. Akta Keselamatan Siber 2024 [Akta 854]
34. Akta Perlindungan Data Peribadi (Pindaan) 2024 [Akta A1727]
35. Akta Perkongsian Data 2025 [Akta 864]
36. Peraturan-Peraturan Keselamatan Siber (Tempoh Bagi Penilaian Risiko Keselamatan Siber dan Audit) 2024 [P.U. (A) 219/2024]
37. Peraturan-Peraturan Keselamatan Siber (Pemberitahuan Insiden Keselamatan Siber) 2024 [P.U. (A) 220/2024]

38. Peraturan-Peraturan Keselamatan Siber (Pelesenan Pemberi Perkhidmatan Keselamatan Siber) 2024 [P.U. (A) 221/2024]
39. Arahan Ketua Eksekutif NACSA No. 1 hingga No. 10
40. Garis Asas Keselamatan Siber Negara (National Cyber Security Baseline - NCSB V1.3)
41. *Buku Panduan Kejuruteraan Sistem Aplikasi Sektor Awam (KRISA) Versi Beta 2026*
42. *CIS Bencmarks*

REKOD PINDAAN DOKUMEN

VERSI	CATATAN KEMASKINI /PINDAAN	TARIKH
2.0	indaan Polisi Keselamatan Siber daripada Versi 1.0 kepada Versi 2.0 selaras dengan keperluan standard ISO/IEC 27001:2022	21 Jul 2024
3.0	Pindaan berdasarkan Tataamalan yang dikeluarkan oleh Jabatan Digital Negara selaku Ketua Sektor Infrastruktur Maklumat Kritikal Negara (NCII). a. Para 4.1: laporan penilaian risiko aset ICT NCII dikemukakan kepada NACSA dan JDN dalam tempoh 30 hari. b. Para 5.1.3 (a) dan (c): semakan PKS sekurang-kurangnya setahun sekali; pindaan minor diluluskan JK ISMS, pindaan major oleh JPICT KPT. c. Para 5.1.4 (b) dan (c): ditambah ketidakpatuhan, pembetulan kawalan tambahan dan tertakluk kepada arahan NACSA serta Akta 854. d. Para 5.2.2, 5.2.3 dan 5.2.4: peranan CDO, ICTSO (melantik tiga (3) individu pemberitahuan insiden) dan JK ISMS ditambah. e. Para 5.2.6: Pengurus CSIRT ditukar daripada "KPSU(M) TK" kepada "KPSU(M) TT". f. Para 5.9: perubahan material aset NCII dimaklumkan kepada JDN dalam tempoh 30 hari. g. Para 5.17 (i): had kata laluan tiga (3) kali berturut-turut. h. Para 5.19 dan 5.35: penyedia SOC, ujian penembusan dan juruaudit dilesenkan/diluluskan NACSA; laporan audit dihantar dalam 30 hari; audit NACSA sekurang-kurangnya sekali dalam dua tahun.	22 Okt 2026

VERSI	CATATAN KEMASKINI /PINDAAN	TARIKH
	i. Para 5.24 dan 6.8 (c): prosedur pelaporan insiden NCII (e-mel NACSA, Portal NC4 dalam 6 jam, maklumat tambahan dalam 14 hari). j. Para 5.30: DRP dan PKP diuji dan disimulasi sekurang-kurangnya setahun sekali. k. Para 8.1: tiga (3) butiran dihapuskan. l. Para 8.12 (d), 8.20 (g), 8.24 (f), 8.26 (f) dan 8.29 (g): integrasi log DLP dengan SIEM, rajah rangkaian terkini, perancangan PQC, pematuhan PCI-DSS dan Ujian Prestasi. m. Bahagian Rujukan, Glosari dan senarai perundangan dikemaskini (Akta 854, Tataamalan JDN v1.3, akronim baharu dan lapan (8) peraturan).	

LAMPIRAN 1

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER KEMENTERIAN PENDIDIKAN TINGGI
(WARGA KPT)

Nama (Huruf Besar) :

No. Kad Pengenalan :

Jawatan :

Bahagian/Unit :

Saya dengan sesungguhnya mengaku bahawa:

1. Saya telah membaca dan memahami Polisi Keselamatan Siber Kementerian Pendidikan Tinggi (PKS KPT) serta bersetuju mematuhi semua peruntukan, terma, syarat dan prosedur keselamatan yang berkuat kuasa dan terpakai kepada saya. Saya akan melaksanakan peranan dan tanggungjawab yang ditetapkan serta melindungi kerahsiaan, integriti dan ketersediaan maklumat dan aset ICT KPT;

2. Saya bertanggungjawab atas akaun dan hak capaian saya, menjaga kerahsiaan maklumat Kerajaan serta segera melaporkan aktiviti atau insiden yang mengancam keselamatan ICT kepada CSIRT KPT. Saya kekal bertanggungjawab dan berakauntabiliti dalam penggunaan AI, tidak memasukkan maklumat yang dilindungi ke dalam perkhidmatan AI yang tidak dibenarkan KPT, serta menyemak dan mengesahkan output AI sewajarnya sebelum digunakan bagi urusan rasmi. Saya memahami bahawa pelanggaran atau ketidakpatuhan PKS KPT boleh mengakibatkan tindakan pembetulan, kawalan keselamatan tambahan atau tindakan tatatertib mengikut peraturan dan perundangan yang berkuat kuasa.

PENGESAHAN PENGGUNA	**PENGESAHAN KETUA BAHAGIAN / ICTSO**
.....	.....
( )	( )
Nama :	b.p. Ketua Setiausaha KPT
Tarikh :	Tarikh :

LAMPIRAN 2

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER KEMENTERIAN PENDIDIKAN TINGGI
(PIHAK KETIGA)

Nama (Huruf Besar) :

No. Kad Pengenalan :

Jawatan :

Syarikat/Organisasi :

Saya dengan sesungguhnya mengaku bahawa:

1. Saya telah membaca dan memahami Polisi Keselamatan Siber Kementerian Pendidikan Tinggi (PKS KPT) serta bersetuju mematuhi semua peruntukan, terma dan syarat yang terpakai kepada saya dan urusan syarikat/organisasi yang saya wakili dengan KPT;

2. Saya akan melaksanakan tanggungjawab pihak ketiga dalam PKS KPT, menjaga kerahsiaan dan melindungi maklumat serta aset ICT KPT yang diakses, diproses atau dikendalikan semasa memberikan perkhidmatan. Saya akan mematuhi keperluan keselamatan dalam perjanjian/kontrak dan perjanjian kerahsiaan serta menandatangani Lampiran E dan Lampiran F di bawah Akta Rahsia Rasmi 1972 (Akta 88) sebagaimana yang ditetapkan dalam PKS KPT; dan

3. Saya bersetuju bahawa pelanggaran PKS KPT oleh saya atau individu yang mewakili syarikat/organisasi ini boleh dikenakan tindakan undang-undang terhadap pihak yang terlibat mengikut undang-undang yang berkuat kuasa. Akuan ini tidak menggantikan perjanjian kerahsiaan atau akuan di bawah Akta Rahsia Rasmi 1972 (Akta 88) yang diperlukan.

PENGESAHAN PENGGUNA	**PENGESAHAN KETUA BAHAGIAN / ICTSO**
.....	.....
( )	( )
Nama :	b.p. Ketua Setiausaha KPT
Tarikh :	Tarikh :