



POLISI KESELAMATAN SIBER

PKPP-ISMS-T2-01

VERSI 1.0

13 NOVEMBER 2025

JADUAL PINDAAN POLISI KESELAMATAN SIBER

TARIKH	VERSI	BUTIRAN PINDAAN

KANDUNGAN

SEJARAH DOKUMEN	ii
TUJUAN.....	1
LATAR BELAKANG.....	1
OBJEKTIF	2
TADBIR URUS.....	3
ASET ICT PKPP	4
RISIKO.....	7
PRINSIP KESELAMATAN.....	9
TEKNOLOGI.....	10
PROSES	13
MANUSIA	15
PELAN PENGURUSAN KESELAMATAN MAKLUMAT	17
A.1 KAWALAN POLISI KESELAMATAN MAKLUMAT (<i>INFORMATION SECURITY POLICY CONTROLS</i>)	18
5.0 KAWALAN ORGANISASI (<i>ORGANIZATIONAL CONTROL</i>).....	18
5.1 POLISI KESELAMATAN MAKLUMAT (<i>POLICIES FOR INFORMATION SECURITY</i>).....	18
5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT (<i>INFORMATION SECURITY ROLES AND RESPONSIBILITIES</i>)	19
5.3 PENGASINGAN TUGAS (<i>SEGREGATION OF DUTIES</i>)	28
5.4 TANGGUNGJAWAB PENGURUSAN (<i>MANAGEMENT RESPONSIBILITIES</i>)	29
5.5 HUBUNGAN DENGAN PIHAK BERKUASA (<i>CONTACT WITH AUTHORITIES</i>)	29
5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS (<i>CONTACT WITH SPECIAL INTEREST GROUPS</i>)	29
5.7 RISIKAN ANCAMAN (<i>THREAT INTELLIGENCE</i>).....	30
5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK (<i>INFORMATION SECURITY IN</i>	

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	iv

<i>PROJECT MANAGEMENT)</i>	30
5.9 INVENTORI MAKLUMAT DAN ASET YANG BERKAITAN (<i>INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS</i>).....	30
5.10 PENGGUNAAN MAKLUMAT DAN ASET BERKAITAN YANG BOLEH DITERIMA (<i>ACCEPTABLE USE OF INFORMATION AND OTHER ASSOCIATED ASSETS</i>)	31
5.11 PEMULANGAN ASET (RETURN OF ASSETS).....	31
5.12 PENGELASAN MAKLUMAT (CLASSIFICATION OF INFORMATION)	32
5.13 PELABELAN MAKLUMAT (LABELLING OF INFORMATION).....	32
5.14 PEMINDAHAN MAKLUMAT (INFORMATION TRANSFER).....	32
5.15 KAWALAN AKSES (ACCESS CONTROL)	34
5.16 PENGURUSAN IDENTITI (IDENTITY MANAGEMENT).....	35
5.17 MAKLUMAT PENGESAHAN (AUTHENTICATION INFORMATION).....	36
5.18 HAK AKSES (ACCESS RIGHT)	36
5.19 KESELAMATAN MAKLUMAT DALAM HUBUNGAN PEMBEKAL (INFORMATION SECURITY IN SUPPLIER RELATIONSHIP).....	36
5.20 MENANGANI KESELAMATAN MAKLUMAT DALAM PERJANJIAN PEMBEKAL (ADDRESSING INFORMATION SECURITY WITHIN SUPPLIER AGREEMENTS).....	37
5.21 PENGURUSAN KESELAMATAN MAKLUMAT DALAM RANTAIAN BEKALAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT) (<i>MANAGING INFORMATION SECURITY IN THE INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SUPPLY CHAIN</i>).....	38
5.22 PEMANTAUAN, SEMAKAN DAN PENGURUSAN PERUBAHAN PERKHIDMATAN PEMBEKAL (MONITORING, REVIEW AND CHANGE MANAGEMENT OF SUPPLIER SERVICES).....	39
5.23 KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN AWAN (INFORMATION SECURITY FOR USE OF CLOUD SERVICES)	39
5.24 PERANCANGAN DAN PERSEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT (INFORMATION SECURITY INCIDENT MANAGEMENT PLANNING AND PREPARATION)	40
5.25 PENILAIAN DAN KEPUTUSAN TENTANG KEJADIAN KESELAMATAN MAKLUMAT (ASSESSMENT AND DECISION ON INFORMATION SECURITY EVENTS)	41
5.26 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT (RESPONSE TO INFORMATION SECURITY INCIDENT)	41
5.27 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT (LEARNING FROM INFORMATION SECURITY INCIDENTS).....	41
5.28 PENGUMPULAN BUKTI (COLLECTION OF EVIDENCE).....	42
5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN (INFORMATION SECURITY DURING DISRUPTION)	42
5.30 KETERSEDIAAN ICT UNTUK KESINAMBUNGAN PERKHIDMATAN (ICT READINESS FOR BUSINESS CONTINUITY).....	43
5.31 KEPERLUAN UNDANG-UNDANG, BERKANUN, PERATURAN DAN KONTRAK (LEGAL, STATUTORY, REGULATORY AND CONTRACTUAL REQUIREMENTS).....	45
5.32 HAK HARTA INTELEK (INTELLECTUAL PROPERTY RIGHTS).....	45
5.33 PERLINDUNGAN REKOD (PROTECTION OF RECORDS)	45
5.34 KERAHSIAAN DAN PERLINDUNGAN MAKLUMAT PENGENALAN PERIBADI (PRIVACY AND PROTECTION OF PERSONAL IDENTIFIABLE INFORMATION (PII)).....	45
5.35 PENILAIAN KESELAMATAN MAKLUMAT OLEH PIHAK BERKECUALI (INDEPENDENT REVIEW OF INFORMATION SECURITY)	45
5.36 PEMATUHAN POLISI, PERATURAN DAN PIAWAIAN KESELAMATAN MAKLUMAT (COMPLIANCE WITH POLICIES, RULES AND STANDARD FOR INFORMATION SECURITY).....	46
5.37 PROSEDUR OPERASI YANG DIDOKUMENKAN (DOCUMENTED OPERATING PROCEDURE)	46

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	v

6.0 KAWALAN MANUSIA (PEOPLE CONTROL)	47
6.1 SARINGAN (SCREENING)	47
6.2 TERMA DAN SYARAT PERJAWATAN (TERMS AND CONDITION EMPLOYMENT)	47
6.3 KESEDARAN, PENDIDIKAN DAN LATIHAN KESELAMATAN MAKLUMAT (INFORMATION SECURITY AWARENESS AND TRAINING)	48
6.4 PROSES TATATERTIB (DISCIPLINARY PROCESS)	48
6.5 TANGGUNGJAWAB SELEPAS PENAMATAN ATAU PERTUKARAN PERJAWATAN (RESPONSIBILITIES AFTER TERMINATION OR CHANGE OF EMPLOYMENT)	49
6.6 PERJANJIAN KERAHSIAAN (CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS)	49
6.7 TELEKERJA (REMOTE WORKING)	50
6.8 PELAPORAN KEJADIAN KESELAMATAN MAKLUMAT (INFORMATION SECURITY EVENT REPORTING)	50
7.0 KAWALAN FIZIKAL (PHYSICAL CONTROL)	52
7.1 PERIMETER KESELAMATAN FIZIKAL (PHYSICAL SECURITY PERIMETERS)	52
7.2 KEMASUKAN FIZIKAL (PHYSICAL ENTRY)	52
7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN (SECURING OFFICES, ROOMS AND FACILITIES)	53
7.4 PEMANTAUAN KESELAMATAN FIZIKAL (PHYSICAL SECURITY MONITORING)	53
7.5 PERLINDUNGAN DARI ANCAMAN FIZIKAL DAN PERSEKITARAN (PROTECTION AGAINST PHYSICAL AND ENVIRONMENTAL THREATS)	53
7.6 BEKERJA DI KAWASAN YANG SELAMAT (WORKING IN SECURE AREA)	54
7.7 MEJA KOSONG DAN SKRIN KOSONG (CLEAR DESK AND CLEAR SCREEN)	54
7.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN (EQUIPMENT SITING AND PROTECTION)	55
7.9 KESELAMATAN ASET DI LUAR PREMIS (SECURITY OF ASSETS OF PREMISES)	57
7.10 MEDIA STORAN (STORAGE MEDIA)	57
7.11 UTILITI SOKONGAN (SUPPORTING UTILITIES)	58
7.12 KESELAMATAN KABEL (CABLING SECURITY)	59
7.13 PENYELENGGARAAN PERKAKASAN (EQUIPMENT MAINTENANCE)	59
7.14 PELUPUSAN SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN (SECURE DISPOSAL OR RE-USE OF EQUIPMENT)	60
8 KAWALAN TEKNOLOGI (TECHNOLOGICAL CONTROL)	62
8.1 PERANTI PENGGUNA (USER END POINT DEVICES)	62
8.2 HAK AKSES ISTIMEWA (PRIVILEGED ACCESS RIGHT)	62
8.3 SEKATAN AKSES MAKLUMAT (INFORMATION ACCESS RESTRICTION)	64
8.4 AKSES KEPADA KOD SUMBER (ACCESS TO SOURCE CODE)	64
8.5 PENGESAHAN KESELAMATAN (SECURE AUTHENTICATION)	64
8.6 PENGURUSAN KAPASITI (CAPACITY MANAGEMENT)	65
8.7 PERLINDUNGAN DARIPADA PERISIAN HASAD (PROTECTION AGAINST MALWARE)	66
8.8 PENGURUSAN KERENTANAN TEKNIKAL (MANAGEMENT OF TECHNICAL VULNERABILITIES)	66
8.9 PENGURUSAN KONFIGURASI (CONFIGURATION MANAGEMENT)	67
8.10 PENGHAPUSAN MAKLUMAT (INFORMATION DELETION)	67
8.11 PELITUPAN DATA (DATA MASKING)	68
8.12 PENCEGAHAN KEBOCORAN DATA (DATA LEAKAGE PREVENTION)	68

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	vi

8.13 SANDARAN MAKLUMAT (<i>INFORMATION BACKUP</i>)	69
8.14 KETERSEDIAAN KEMUDAHAN PEMROSESAN MAKLUMAT (<i>REDUNDANCY OF INFORMATION PROCESSING FACILITIES</i>)	70
8.15 LOGGING (<i>LOGGING</i>).....	70
8.16 AKTIVITI PEMANTAUAN (<i>MONITORING ACTIVITIES</i>)	71
8.17 PENYEGERAKAN JAM (<i>CLOCK SYNCHRONISATION</i>)	71
8.18 PENGGUNAAN UTILITI PROGRAM ISTIMEWA (<i>USE OF PRIVILEGED UTILITY PROGRAMS</i>)	72
8.19 PEMASANGAN PERISIAN PADA SISTEM OPERASI (<i>INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS</i>).....	73
8.20 KESELAMATAN RANGKAIAN (<i>NETWORKS SECURITY</i>).....	73
8.21 KESELAMATAN PERKHIDMATAN RANGKAIAN (<i>SECURITY OF NETWORK SERVICES</i>)	75
8.22 PENGASINGAN RANGKAIAN (<i>SEGREGATION OF NETWORKS</i>).....	75
8.23 PENAPISAN LAMAN WEB (<i>WEB FILTERING</i>).....	75
8.24 PENGGUNAAN KRIPTOGRAFI (<i>USE OF CRYPTOGRAPHY</i>)	76
8.25 KITARAN HAYAT PEMBANGUNAN SELAMAT (<i>SECURE DEVELOPMENT LIFE CYCLE</i>)	76
KEPERLUAN KESELAMATAN APLIKASI (<i>APPLICATION</i>	77
8.26 <i>SECURITY REQUIREMENTS</i>)	77
PRINSIP SENIBINA DAN KEJURUTERAAN SISTEM SELAMAT	78
8.27 (<i>SECURE SYSTEM ARCHITECTURES AND ENGINEERING PRINCIPLES</i>).....	78
8.28 PENGKODAN SELAMAT (<i>SECURE CODING</i>).....	78
8.29 PENGUJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN (<i>SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE</i>)	79
8.30 PEMBANGUNAN OLEH PIHAK LUAR (<i>OUTSOURCED DEVELOPMENT</i>).....	79
PENGASINGAN PERSEKITARAN PEMBANGUNAN , PENGUJIAN DAN OPERASI	80
8.31 (<i>SEPARATION OF DEVELOPMENT, TEST AND PRODUCTION ENVIRONMENT</i>).....	80
8.32 PENGURUSAN PERUBAHAN (<i>CHANGE MANAGEMENT</i>).....	81
8.33 MAKLUMAT UJIAN (<i>TEST INFORMATION</i>).....	82
8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PENGUJIAN AUDIT (<i>PROTECTION OF INFORMATION SYSTEMS DURING AUDIT TESTING</i>).....	82
 GLOSARI	 83
 LAMPIRAN 1: SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER PKPP PAHANG	 88
 LAMPIRAN 2: SURAT PERAKUAN PEMATUHAN AKTA RAHSIA RASMI 1972 [AKTA 88] DAN POLISI KESELAMATAN SIBER PKPP	 87
 LAMPIRAN 3 : PROSES KERJA PELAPORAN INSIDEN KESELAMATAN SIBER PKPP	
 LAMPIRAN 4 : SENARAI PERUNDANGAN DAN PERATURAN	 90

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	vii

TAKRIFAN

1. Anti virus Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, optical disk, flash disk, CDROM untuk sebarang kemungkinan adanya virus.
2. Aset ICT Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
3. Aset Alih Aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
4. *Backup* (Sandaran) Proses penduaan sesuatu dokumen atau maklumat
5. Baki risiko Risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan.
6. *Bandwidth* Lebar Jalur
7. BCP/PKP *Business Continuity Planning* / Pelan Kesenambungan Perkhidmatan
8. CCTV *Closed-Circuit Television System*
Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
9. CIA *Confidentiality, Integrity, Availability*
10. CDO *Chief Digital Officer*
Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan maklumat digital bagi menyokong arah tuju sesebuah organisasi.
11. *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.
12. *Denial of service* Halangan pemberian perkhidmatan
13. *Defence-in-depth* Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.
14. *Downloading* Aktiviti muat turun sesuatu perisian.
15. *Encryption* Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
16. *Escrow* (eskrow) Sebarang sistem yang membuat salinan kunci penyulitan supaya boleh dicapai oleh individu yang dibenarkan pada bila-bila masa.
17. *Forgery* Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*) dan penipuan (*hoaxes*).
18. CSIRT PKPP *Cyber Security and Incident Response Teams* atau Pasukan Tindak Balas Keselamatan Siber PKPP.
19. *Hard disk* Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
20. *Hub* Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	1

(broadcast) data yang diterima daripada sesuatu port kepada semua port yang lain.

21. *ICT* *Information and Communication Technology*
Teknologi Maklumat dan Komunikasi
22. *ICTSO* *ICT Security Officer*
Pegawai yang bertanggungjawab terhadap keselamatan siber.
23. Impak teknikal Melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti.
24. BTM Bahagian Teknologi Maklumat
25. BPSM Bahagian Pentadbiran dan Sumber Manusia

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	1

TUJUAN

Polisi Keselamatan Siber, Perbadanan Kemajuan Pertanian Negeri Pahang (PKPP) ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh kakitangan PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP dalam melindungi maklumat di ruang siber.

LATAR BELAKANG

Polisi ini dibangunkan untuk menjamin kesinambungan urusan PKPP dengan meminimumkan kesan insiden keselamatan siber. Polisi ini akan memudahkan perkongsian maklumat sesuai dengan keperluan operasi PKPP bagi memastikan semua maklumat dilindungi.

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	1

OBJEKTIF

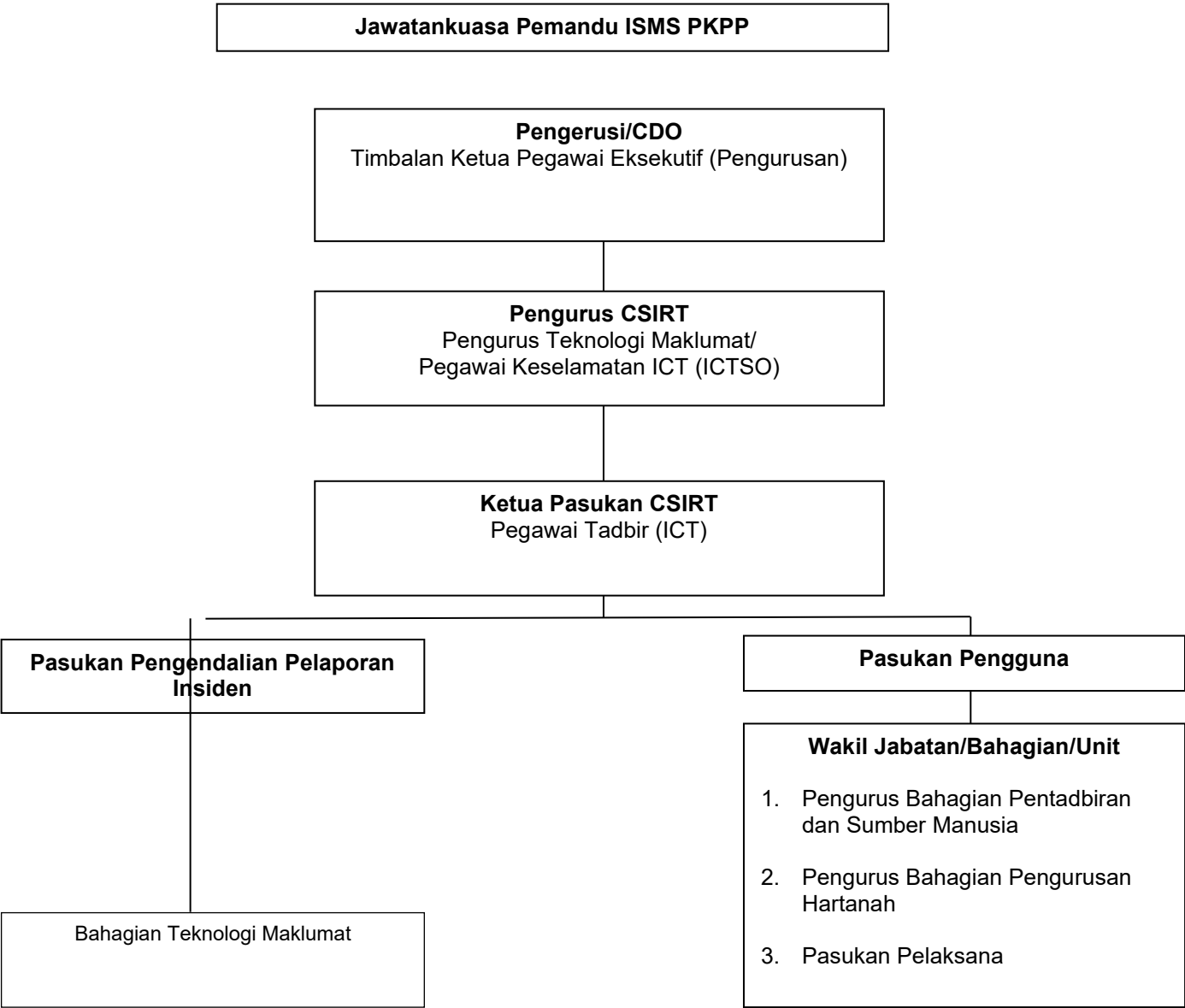
Objektif utama Polisi Keselamatan Siber ini dibangunkan adalah seperti yang berikut:

- a. Menerangkan kepada semua pengguna merangkumi warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber.
- b. Memastikan keselamatan penyampaian perkhidmatan PKPP di tahap tertinggi sekali gus meningkatkan tahap keyakinan pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;
- c. Memastikan kelancaran operasi PKPP dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;
- d. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan yang berlaku dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan
- e. Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	2

TADBIR URUS

Bagi memastikan keberkesanan dan kejayaan pelaksanaan PKS PKPP, satu (1) struktur tadbir urus iaitu Jawatankuasa Pemandu ISMS PKPP telah diwujudkan seperti berikut:



RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	3

Keahlian Jawatankuasa ini adalah seperti yang berikut:

Ketua: CDO (Timbalan Ketua Pegawai Eksekutif (Pengurusan))

Ahli:

- a. Pengurus Teknologi Maklumat
- b. Pengurus bahagian-bahagian yang terlibat dengan skop ISMS
- c. Pasukan Pelaksana ISMS
- d. Urusetia ISMS

Peranan Jawatankuasa adalah berkaitan:

- a. Pelaksanaan pensijilan ISMS ke atas perkhidmatan PKPP yang dikenal pasti;
- b. Kelulusan ke atas dasar, objektif dan skop pelaksanaan ISMS;
- c. Penetapan kriteria penerimaan risiko, tahap risiko dan pelan penguraian risiko;
- d. Keputusan dan tindakan Mesyuarat Jawatankuasa Pelaksana ISMS;
- e. Kajian semula pelaksanaan pensijilan ISMS ke atas perkhidmatan-perkhidmatan PKPP yang dikenal pasti;
- f. Dasar dan objektif ISMS diwujudkan selaras dengan hala tuju strategik PKPP;
- g. Keperluan ISMS diterapkan dalam budaya kerja pegawai PKPP;
- h. Sumber yang diperlukan oleh pasukan pelaksana ISMS;
- i. Kepentingan pengurusan ISMS yang berkesan dan pematuhan terhadap keperluannya;
- j. Pencapaian sasaran ISMS seperti yang dirancang;
- k. Arahan dan sokongan kepada Pasukan ISMS PKPP bagi memastikan ISMS dapat dilaksanakan dengan berkesan; dan
- l. Pelaksanaan program penambahbaikan dan peningkatan ISMS yang berterusan.

ASET ICT PKPP

Polisi ini meliputi semua sumber atau aset ICT yang digunakan seperti :

- a. Maklumat
 - i. Semua penyedia perkhidmatan dalam PKPP hendaklah mengenalpasti maklumat yang dijana dan hendaklah mengasingkannya mengikut kategori:

1. Maklumat Rahsia Rasmi - Di bawah Akta Rahsia Rasmi 1972 (Akta 88), maksud

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	4

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.

2. Maklumat Rasmi - maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh PKPP semasa menjalankan urusan rasmi. Maklumat rasmi ini juga merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara.

3. Maklumat Pengenalan Peribadi - Maklumat Pengenalan Peribadi (PII atau Personally Identifiable Information) ialah maklumat yang boleh digunakan secara tersendiri atau digunakan bersama maklumat lain untuk mengenalpasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu. PII boleh juga terkandung dalam Maklumat Rahsia Rasmi.

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

b. Aliran Data

i. Aliran data merujuk kepada laluan lengkap data tertentu semasa transaksi. Aliran data dan komunikasi dalam PKPP hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Saluran komunikasi termasuk:

1. Saluran komunikasi dan aliran data antara sistem di PKPP;
2. Saluran komunikasi dan aliran data ke sistem luar; dan

Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.

c. Platform Aplikasi dan Perisian

i. Semua platform aplikasi dan perisian hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

d. Peranti Fizikal dan Sistem

i. Semua peranti fizikal dan sistem hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Peranti fizikal termasuk:

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	5

1. Pelayan;
2. Peranti/Peralatan Rangkaian;
3. Komputer Peribadi/Komputer Riba;
4. Telefon/peranti pintar;
5. Media Storan;
6. Peranti dengan sambungan ke rangkaian, contohnya pengimbas, mesin pencetak, sistem kawalan akses, alat kawalan dan sistem kamera litar tertutup (CCTV);
7. Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi PKPP; dan
8. Peranti pengesahan (authentication devices), contohnya token keselamatan, dongle dan alat pengimbas biometrik.

e. Sistem Luaran

- i. Sistem luaran ialah sistem bukan milik PKPP yang dihubungkan dengan sistem PKPP. Semua sistem luaran hendaklah dikenal pasti, direkodkan dan dinilai tahap keselamatannya secara berkala.

f. Sumber Luaran

- i. Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkod dan dinilai tahap keselamatannya secara berkala. Perkhidmatan sumber luaran ialah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi PKPP. Contoh perkhidmatan sumber luaran ialah:
 1. Perisian Sebagai Satu Perkhidmatan
 2. Platform Sebagai Satu Perkhidmatan
 3. Infrastruktur Sebagai Satu Perkhidmatan
 4. Storan Pengkomputeran Awan
 5. Pemantauan Keselamatan
- ii. Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan, dikaji semula dan dipastikan keselamatannya secara berkala.

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

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	6

RISIKO

PKPP hendaklah mengenal pasti risiko yang berkaitan dengan maklumat yang terlibat. Risiko ialah kebarangkalian PKPP tidak dapat melaksanakan fungsi jabatan dengan baik. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam ruang siber PKPP.

Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran siber PKPP .

Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

a. Kerentanan

Kerentanan adalah kelemahan atau kecacatan aset yang mungkin dieksploitasi dan mengakibatkan pelanggaran keselamatan. Kerentanan setiap aset hendaklah dikenal pasti sebagai sebahagian daripada proses pengurusan risiko.

b. Ancaman

PKPP hendaklah mengenalpasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

c. Impak

PKPP hendaklah menganggarkan impak insiden yang mungkin terjadi. Impak boleh dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi PKPP.

d. Tahap Risiko

Tahap risiko ditentukan daripada ancaman, kebarangkalian dan impak risiko. Kaedah penentuan hendaklah mengikut polisi penilaian atau pengurusan risiko yang sedang berkuat kuasa.

e. Penguraian Risiko

Penguraian risiko hendaklah dikenal pasti untuk menentukan sama ada risiko perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/faedahnyanya.

Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala dengan mengambil kira perkara berikut:

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	7

1. Teknologi

Teknologi hendaklah dikenal pasti untuk mengurangkan risiko. Sebagai contoh, tembok api digunakan untuk mengehadkan capaian logikal kepada sistem tertentu.

2. Proses

Perekayasaan proses, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

3. Manusia

Mengenalpasti sumber manusia berkecukupan dan kompeten yang mencukupi serta memastikan pengurusan sumber manusia dilaksanakan sebagai pengolahan risiko yang berkesan.

f. Pengurusan Risiko

1. Penyedia perkhidmatan digital di PKPP hendaklah memastikan tadbir urus pengurusan risiko diwujudkan dengan mengambil kira perkara berikut:

- i. mengenalpasti kerentanan;
- ii. mengenalpasti ancaman;
- iii. menilai risiko;
- iv. menentukan penguraian risiko;
- v. memantau keberkesanan penguraian risiko; dan
- vi. memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

2. Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya sekali setahun oleh Jawatankuasa Pelaksana ISMS dan dimaklumkan kepada Mesyuarat Jawatankuasa Pemandu ISMS PKPP.

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	8

PRINSIP KESELAMATAN

Prinsip-prinsip yang menjadi asas kepada Polisi Keselamatan Siber PKPP dan perlu dipatuhi adalah seperti berikut:

a. Prinsip “Perlu-Tahu”

PKPP hendaklah melaksanakan mekanisme bagi memberikan kebenaran kepada capaian maklumat. Maklumat yang dicapai oleh pengguna yang dibenarkan hendaklah berdasarkan prinsip “Perlu-Tahu” yang membenarkan capaian maklumat yang diperlukan untuk melaksanakan tugasnya sahaja.

Bagi capaian spesifik Maklumat Rahsia Rasmi, penggunaan yang dibenarkan hendaklah dihadkan kepada masa, lokasi, peranan dan fungsi pengguna tersebut.

b. Hak Keistimewaan minimum

Pengguna hendaklah diberikan hak keistimewaan minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujudkan, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Prinsip ini digunakan untuk menyekat hak akses kepada aplikasi, sistem, proses dan peranti kepada pengguna yang dibenarkan untuk melaksanakan aktiviti. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

c. Pengasingan Tugas

Bagi mengekalkan prinsip sekat-dan-imbang (check and balance), PKPP hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

d. Kawalan Capaian Berdasarkan Peranan

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

e. Peminimuman Data

PKPP hendaklah mengamalkan prinsip peminimuman data yang mengehadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	9

TEKNOLOGI

Teknologi untuk melindungi data hendaklah dikenal pasti di semua peringkat pemprosesan data di setiap elemen pengkomputeran seperti berikut:

a. Peringkat Pemprosesan Data

1. Data-dalam-simpanan

- i. PKPP hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-simpanan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-simpanan.
- ii. Maklumat Rahsia Rasmi, Maklumat Rasmi dan PII perlu dilindungi daripada segi kerahsiaan dan integriti data. Data terbuka perlu dilindungi daripada segi integriti data.

2. Data-dalam-pergerakan

PKPP hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-pergerakan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data- dalam-pergerakan.

3. Data-dalam-penggunaan

- i. PKPP hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-penggunaan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Di samping itu, teknologi untuk menentukan asal data dan tanpa sangkalan mungkin diperlukan. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data dalam penggunaan.
- ii. Teknologi yang bersesuaian boleh digunakan untuk memastikan keaslian data dan data/transaksi tanpa-sangkal.

4. Perlindungan Ketirisan Data

- i. Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.
- ii. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	10

b. Elemen Dalam Persekitaran Pengkomputeran

Berdasarkan penilaian risiko dan pelan pengurusan risiko, PKPP hendaklah menggunakan kaedah teknologi dan kawalan keselamatan (*countermeasure and control measure*) yang dapat melindungi data di semua peringkat saluran pemprosesan bagi semua elemen dalam persekitaran pengkomputeran.

Maklumat Terkawal (Rahsia Rasmi) hendaklah disimpan dan diproses dalam persekitaran pengh komputeran mengikut Prosedur Kawalan Keselamatan Dokumen PKPP yang dikeluarkan oleh PKPP.

Setiap projek ICT yang dibangunkan di PKPP dan menyimpan maklumat terkawal hendaklah mempunyai Pelan Pengurusan Keselamatan Maklumat tersendiri yang mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

1. Peranti pengkomputeran peribadi
 - i. Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, stesen kerja dan peranti storan.
 - ii. Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Terkawal hendaklah memohon kebenaran daripada pihak bertanggungjawab di PKPP.
2. Peranti rangkaian
 - i. merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti suis, penghala, tembok api, peranti VPN dan kabel.
 - ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.
3. Aplikasi
 - i. Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi, sistem operasi.
 - ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	11

4. Pelayan

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

5. Persekitaran fizikal

- i. Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.
- ii. PKPP hendaklah merujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.
- iii. Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip *defence-in-depth*.
- iv. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	12

PROSES

Warga PKPP hendaklah melindungi keselamatan siber dengan melaksanakan perkara-perkara berikut:

- a. Konfigurasi Asas
 1. Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi prasyarat pentauliahkan sistem.
 2. Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan.
- b. Kawalan Perubahan Konfigurasi
 1. Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.
 2. Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asas terkini.
 3. Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan.
- c. Sandaran
 1. Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang sedang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan.
 2. Media sandaran hendaklah disimpan dalam persekitaran yang selamat dan di lokasi yang berasingan.
- d. Kitaran Pengurusan Aset
 1. **Pindah**
 - i. Pemindahan hak milik aset berlaku dalam keadaan berikut:
 - a) Warga PKPP meninggalkan agensi disebabkan oleh persaraan, perletakan jawatan atau penugasan semula;
 - b) Aset yang dikongsi untuk kegunaan sementara;
 - c) Pemberian aset kepada agensi lain; dan
 - d) Aset dikembalikan setelah tamat tempoh sewaan.
 - ii. Data dalam peranti tersebut hendaklah diuruskan mengikut tatacara pelupusan di perkara (2).

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	13

2. Pelupusan

- i. Pelupusan media storan hendaklah dirujuk kepada CGSO sebagai langkah pertama di mana CGSO akan membuat keputusan sama ada sistem itu mengandungi maklumat terperingkat atau sebaliknya.
- ii. Berdasarkan keputusan CGSO, pelupusan perlu dirujuk kepada Arkib Negara Malaysia bagi semakan sama ada sistem itu mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara 2003 (Akta 629) dan Warta Kerajaan P.U.(A)377. Peraturan-Peraturan Arkib Negara (Penetapan Borang-Borang bagi Pelupusan Rekod Awam) 2008.
- iii. Pelupusan boleh dalam bentuk pemusnahan fizikal dan/atau sanitasi data.
- iv. Sanitasi data hendaklah mengikut Garis Panduan Sanitasi Media Elektronik Sektor Awam yang sedang berkuat kuasa.

3. Kitaran Hayat

- i. Kitaran hayat data hendaklah diuruskan mengikut Akta 629.
- ii. Akta 629 memberikan mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umum selama lima tahun.

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	14

MANUSIA

Warga PKPP, pembekal, pakar runding dan pihak-pihak yang berkepentingan hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.

Sistem penyampaian perkhidmatan Kerajaan hendaklah dikendalikan oleh individu yang kompeten dan berpengetahuan. Kakitangan hendaklah dilatih dalam bidang pengkhususan yang diperlukan. Asas kecekapan pengguna hendaklah dibangunkan bagi semua warga PKPP.

a. Kompetensi pengguna

1. Kompetensi pengguna termasuk:

- i. Kesedaran amalan terbaik keselamatan maklumat dengan memupuk amalan baik keselamatan siber dengan mewujudkan komunikasi ICT dan program kesedaran keselamatan siber.
- ii. Kemahiran menggunakan alat keselamatan dengan menyediakan latihan yang mencukupi kepada warga PKPP berhubung alat-alat keselamatan berkaitan untuk memastikan mereka mampu untuk melaksanakan tugas harian mereka.
- iii. Kompetensi pengguna hendaklah tertakluk kepada penilaian berkala melalui ujian khusus.
- iv. Setiap orang yang diberi kuasa untuk mengendalikan dokumen terperingkat, kompetensi tambahan pengguna selaras dengan arahan/pekeling semasa adalah diharapkan.

b. Kompetensi pelaksana

1. Warga PKPP yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.
2. Pegawai Keselamatan ICT hendaklah memenuhi syarat-syarat berikut:
 - i. Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber.
 - ii. Memenuhi keperluan pembelajaran berterusan.
 - iii. Menimba pengalaman yang mencukupi dalam bidang keselamatan siber.
 - iv. Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa.

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	15

3. Pegawai Keselamatan ICT yang dilantik hendaklah memenuhi keperluan kompetensi di atas. Pegawai Keselamatan ICT bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan di PKPP.

c. Peranan

1. Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna.
2. Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka.
3. Warga PKPP yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT dikembalikan sekiranya berlaku perubahan peranan.
4. Warga PKPP yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan yang berkaitan seperti tersenarai dalam senarai aset dalam Nota Serah Tugas.
5. Warga PKPP yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan dengan diselia oleh kakitangan yang dipertanggungjawabkan.

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 4.0	15/01/2025	16

PELAN PENGURUSAN KESELAMATAN MAKLUMAT

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

Pernyataan ini merangkumi perlindungan semua bentuk maklumat elektronik dan bukan elektronik yang dimasukkan, diwujudkan, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan bagi memelihara keselamatan ruang siber dan ketersediaan maklumat kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

a. Kerahsiaan

Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.

b. Integriti

Data dan maklumat hendaklah tepat, lengkap dan kemas kini dan hanya boleh diubah dengan cara yang dibenarkan.

c. Tidak Boleh Disangkal

Punca data dan maklumat hendaklah daripada punca 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.

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

Empat (4) kawalan yang terlibat di dalam Polisi Keselamatan Siber PKPP diterangkan dengan lebih jelas dan teratur dalam dokumen ini.

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	17

A.1 KAWALAN POLISI KESELAMATAN MAKLUMAT (<i>INFORMATION SECURITY POLICY CONTROLS</i>)	
5.0 KAWALAN ORGANISASI (<i>ORGANIZATIONAL CONTROL</i>)	
5.1 POLISI KESELAMATAN MAKLUMAT (<i>POLICIES FOR INFORMATION SECURITY</i>)	PERANAN
1) Pelaksanaan Polisi ini akan dijalankan oleh PKPP dengan disokong oleh Jawatankuasa ISMS terdiri daripada: i) Pengerusi JK Pemandu ISMS ii) Pegawai Keselamatan ICT (ICTSO) iii) Pengurus-Pengurus Bahagian iv) Ahli-ahli yang dilantik Polisi ini perlu disebarikan dan dipatuhi oleh semua warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP. Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak Pengurusan Teraju PKPP kepada warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP. 2) Polisi Keselamatan Siber ini adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, polisi kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berkaitan dengan kajian semula Polisi Keselamatan Siber PKPP: a. Kenal pasti dan tentukan perubahan yang diperlukan; b. Kemuka cadangan pindaan secara bertulis untuk pembentangan dan persetujuan Mesyuarat Teraju PKPP bagi tujuan pengesahan; c. Maklum kepada semua warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP berkenaan pindaan yang telah diluluskan; dan Polisi ini hendaklah dikaji semula sekurang-kurangnya LIMA (5) tahun sekali atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	Pengurusan Teraju Pengurusan Teraju/CDO/ICTSO

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	18

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT (INFORMATION SECURITY ROLES AND RESPONSIBILITIES)	PERANAN
5.2.1 Peranan dan tanggungjawab Ketua Pegawai Eksekutif adalah seperti berikut: - Memastikan penguatkuasaan pelaksanaan Polisi ini; - Memastikan semua warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini; - Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; dan - Memastikan pengurusan risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam Polisi ini; dan - Melantik CDO dan ICTSO.	Ketua Pegawai Eksekutif
5.2.2 Timbalan Ketua Pegawai Eksekutif (Pengurusan) adalah merupakan Ketua Pegawai Digital (CDO). Peranan dan tanggungjawab beliau adalah seperti berikut: - Membantu Ketua Pegawai Eksekutif dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber seperti yang ditetapkan dalam Polisi ini; - Memastikan kawalan keselamatan maklumat dalam PKPP diseragam dan diselaraskan dengan sebaiknya; - Memastikan Pelan Strategik PKPP (program Pendigitalan) mengandungi aspek keselamatan siber; dan - Menyelaras pelan latihan dan program kesedaran keselamatan siber.	Ketua Pegawai Digital (CDO)
5.2.3 Pengurus Teknologi Maklumat adalah merupakan ICTSO PKPP. Peranan dan tanggungjawab ICTSO adalah seperti berikut : - Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini; - Merangka pengurusan risiko dan audit keselamatan siber berpandukan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat yang berkuat kuasa; - Menyedia dan menyebarkan amaran-amaran yang sesuai	ICTSO

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	19

terhadap kemungkinan berlakunya ancaman keselamatan siber dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; d. Melaporkan insiden keselamatan siber kepada Agensi Keselamatan Siber Negara (NACSA), Majlis Keselamatan Negara dan seterusnya membantu dalam penyiasatan atau pemulihan. e. Melaporkan insiden kepada CDO bagi insiden yang memerlukan Pengurusan Kesenambungan Perkhidmatan (PKP); f. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera; g. Melaksanakan pematuhan Polisi ini oleh warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP; h. Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber; dan i. Menyedia dan merangka latihan dan program kesedaran keselamatan siber. j. Menjadi Pengurus CSIRT PKPP.	ICTSO
5.2.4 Semua Pengurus Bahagian/Ketua Unit di PKPP berperanan dan bertanggungjawab dalam melaksanakan keperluan Polisi ini dalam operasi semasa bahagian/unit seperti yang berikut: a. Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu; b. Pembelian atau peningkatan perisian dan sistem komputer; c. Perolehan teknologi dan perkhidmatan komunikasi baru; d. Menentukan pembekal dan rakan usaha sama menjalani tapisan keselamatan; dan e. Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat kerajaan yang berkuat kuasa.	Pengurus Bahagian/Ketua Unit

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	20

5.2.5 Peranan dan tanggungjawab Pentadbir Sistem Aplikasi/Perkhidmatan Digital adalah seperti berikut:

- a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;
- b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di 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 memberhentikanannya dengan serta merta;
- e. Menganalisis dan menyimpan rekod jejak audit;
- f. Menyediakan laporan mengenai aktiviti capaian secara berkala;
- g. Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas;
- h. Memastikan kod-kod program sistem aplikasi adalah selamat daripada penggadam sebelum sistem tersebut diaktifkan penggunaannya;
- i. Memastikan *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi dikemaskini supaya terhindar daripada ancaman virus dan penggadam;
- j. Mematuhi dan melaksanakan prinsip-prinsip Polisi ini dalam penwujudan akaun pengguna ke atas setiap sistem aplikasi;
- k. Memastikan backup sistem aplikasi dan data yang berkaitan dengannya dibuat secara berjadual;
- l. Menghadkan capaian Dokumentasi Sistem Aplikasi bagi mengelakkan dari penyalahgunaannya;
- m. Melaporkan kepada CSIRT PKPP jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya;

Pentadbir Sistem
Aplikasi/Perkhidmatan Digital

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	21

5.2.6 Peranan dan tanggungjawab Pentadbir Teknikal adalah seperti berikut : - Menyediakan khidmat sokongan teknikal ICT; - Merancang dan melaksanakan perolehan aset ICT; - Mengurus pendaftaran, agihan, penempatan dan pelupusan Aset ICT; - Memastikan semua aset ICT diselenggarakan secara berkala dengan sempurna; - Memastikan perisian antivirus dipasang pada Aset ICT; dan - Mengurus Meja Bantuan ICT PKPP.	Pentadbir Teknikal
5.2.7 Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut : - Memastikan rangkaian setempat (LAN), rangkaian luas (WAN) dan rangkaian PKPP beroperasi sepanjang masa; - Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna; - Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; - Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidakstabil dan sebarang kerosakan perkakasan sokongan rangkaian PKPP; - Memantau penggunaan rangkaian dan melaporkan kepada CSIRT PKPP sekiranya berlaku penyalahgunaan sumber rangkaian; - Mewartakan polisi dan garis panduan penggunaan rangkaian PKPP kepada pengguna rangkaian; - Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan luar ke dalam rangkaian PKPP secara tidak sah; dan	Pentadbir Rangkaian

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	

5.2.8 Peranan dan tanggungjawab pentadbir Laman Web adalah seperti berikut: - Menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah; - Memantau prestasi capaian dan menjalankan penalaan prestasi untuk memastikan akses yang lancar; - Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, mencero boh dan mengubahsuai muka laman; - Menghadkan capaian Pentadbir Laman Web bahagian/unit ke web server; - Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; - Melaporkan sebarang pelanggaran keselamatan laman portal kepada CSIRT PKPP.	Pentadbir Laman Web/portal (WEBMASTER)
5.2.9 Peranan dan tanggungjawab pentadbir E-Mel adalah seperti berikut: - Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan oleh Pengurus Teknologi Maklumat. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar Polisi dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; - Pentadbir e-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib; - Menyimpan jejak audit selama sekurang-kurangnya enam (6) bulan di dalam pelayan e-mel ATAU tertakluk kepada kemampuan ruang storan; - Melaksanakan jadual penstoran dan mengarkibkan e-mel. Penyimpanan media storan sama ada di luar atau di dalam kawasan mestilah mempunyai ciri-ciri keselamatan fizikal yang terjamin bagi mengelak daripada sebarang risiko seperti kehilangan maklumat; - Memastikan akaun e-mel pengguna sentiasa dalam keadaan baik dan berfungsi; - Memastikan keselamatan akaun e-mel pengguna dari ancaman luar dan dalam;	Pentadbir E-Mel

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	23

g. Melaksanakan penyelenggaraan ke atas sistem e-mel dengan baik dan menentukan segala <i>patches</i> terkini yang disediakan oleh pihak pembekal dipasang dan berfungsi dengan sempurna; h. Memantau status storan e-mel Pengurusan Atasan PKPP dan memastikan emel Pengurusan Atasan PKPP sentiasa tersedia untuk transaksi e-mel; i. Memastikan semua peralatan sistem e-mel sentiasa aktif 24 x 7; j. Memastikan agar keupayaan mail relay hanya boleh digunakan untuk server atau aplikasi dalaman PKPP sahaja bagi tujuan keselamatan; k. Memastikan kemudahan membuat capaian e-mel melalui pelbagai media seperti telefon mudah alih disediakan kepada pengguna e-mel PKPP; dan l. Memastikan pengguna e-mel PKPP berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel PKPP dan Internet serta pelaksanaan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan melalui latihan serta promosi.	Pentadbir E-Mel
5.2.10 Peranan dan tanggungjawab pegawai aset ICT adalah seperti berikut : a. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya dalam keadaan yang baik; b. Memastikan Aset ICT milik PKPP dilabel dan direkodkan ke dalam Sistem Pengurusan Aset; c. Memastikan Aset milik PKPP dibuat pemeriksaan berkala secara tahunan dan diselenggara sebaiknya agar dapat meningkatkan jangka hayat Aset ICT tersebut; d. Memastikan Aset ICT untuk pinjaman dan simpanan sebelum agihan diletakkan di dalam bilik stor yang mempunyai kawalan keselamatan yang terjamin; e. Memastikan Stok alat ganti Aset ICT sentiasa mencukupi dan disimpan di tempat yang selamat dan terkawal; dan f. Memastikan Aset ICT yang ingin dilupuskan dilaksanakan	Pegawai Aset ICT (Juriah Mohamad)

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	24

mengikut garis panduan kawalan keselamatan bagi pelupusan data digital.	
5.2.11 Peranan dan tanggungjawab pegawai adalah seperti berikut : - Memastikan operasi Pusat Data dan DRC berada dalam keadaan baik 24 x 7; - Merancang dan menyelia pelaksanaan simulasi <i>Disaster Recovery Plan</i> (DRP) PKPP; - Mengurus operasi DRC sekiranya berlaku bencana terhadap Pusat Data PKPP; - Memastikan operasi Infrastruktur pelayan di Pusat Data dan DRC berfungsi dan diselenggara dengan baik bagi meningkatkan jangka hayat perkhidmatan perkakasan serta perisian; - Memastikan operasi <i>backup / restore</i> data berfungsi dan diselenggara dengan baik bagi meningkatkan jangka hayat perkhidmatan perkakasan serta perisian; - Memantau aset ICT sokongan dan fasiliti sokongan (Precision Aircond, Alat Pencegah Kebakaran, Bekalan Elektrik) di Pusat Data dan DRC bagi memastikan beroperasi lancar 24 x 7; - Menguruskan permohonan baru dan pengemaskinian server bagi sistem aplikasi baru di Pusat Data dan DRC; - Melaksanakan <i>housekeeping</i> keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di web server; dan pusat data; dan - Menguruskan khidmat sokongan operasi server dari segi penerimaan, penyediaan, penyelenggaraan, waranti, pengeluaran dan pelupusan.	Pentadbir Pusat Data dan Disaster Recovery Center (DRC)
5.2.12 Peranan dan tanggungjawab Jawatankuasa ISMS adalah seperti berikut: - Menentukan hala tuju keseluruhan pelaksanaan pensijilan ISMS PKPP yang merangkumi perancangan, pemantauan dan pengesahan terhadap perkara-perkara berikut: - Pelaksanaan pensijilan ISMS ke atas perkhidmatan PKPP yang dikenalpasti;	Jawatankuasa Pemandu ISMS

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	25

ii. Kelulusan ke atas dasar, objektif, dan skop pelaksanaan ISMS; dan iii. Penetapan kriteria penerimaan risiko, tahap risiko dan <i>risk treatment plan</i>. b. Keputusan dan tindakan Mesyuarat Jawatankuasa Kerja ISMS PKPP; c. Kajian semula pelaksanaan pensijilan ISMS ke atas perkhidmatan-perkhidmatan PKPP yang dikenal pasti; d. Dasar dan objektif ISMS diwujudkan selaras dengan hala tuju strategik PKPP; e. Keperluan ISMS diterapkan dalam budaya kerja warga kerja PKPP; f. Sumber yang diperlukan oleh pasukan pelaksana ISMS; g. Kepentingan pengurusan ISMS yang berkesan dan pematuhan terhadap keperluannya; h. Pencapaian sasaran ISMS seperti yang dirancang; i. Arahan dan sokongan kepada pasukan ISMS PKPP bagi memastikan ISMS dapat dilaksanakan dengan berkesan; dan j. Pelaksanaan program penambahbaikan dan peningkatan ISMS yang berterusan. Meluluskan: a. Struktur Organisasi ISMS PKPP; b. Keperluan sumber; dan c. Pelantikan Pasukan Audit Dalam ISMS PKPP.	Jawatankuasa Pemandu ISMS
5.2.13 Peranan dan Tanggungjawab CSIRT adalah seperti berikut : a. Menerima dan mengesan aduan keselamatan siber dan menilai tahap dan jenis insiden; b. Merekodkan dan menjalankan siasatan awal insiden yang diterima;	Pasukan CSIRT PKPP

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	26

c. Menangani tindak balas (<i>response</i>) insiden keselamatan siber dan mengambil tindakan baik pulih minima; d. Menghubungi dan melaporkan insiden yang berlaku kepada NACSA sama ada sebagai input atau untuk tindakan seterusnya; e. Menasihatkan agensi-agensi di bawah kawalannya mengambil tindakan pemulihan dan pengukuhan; f. Menyebarkan maklumat berkaitan pengukuhan keselamatan siber kepada agensi di bawah kawalannya; dan g. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	Pasukan CSIRT PKPP
5.2.14 Peranan dan tanggungjawab pengguna adalah seperti berikut: a. Membaca, memahami dan mematuhi Polisi ini; b. Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya; c. Menjalani tapisan keselamatan sekiranya diperlukan dikehendaki berurusan dengan maklumat rasmi terperingkat; d. Mematuhi prinsip-prinsip Polisi ini dan menjaga kerahsiaan maklumat PKPP; e. Melaksanakan langkah-langkah perlindungan seperti berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan siber yang ditetapkan; vi. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan bagi setiap langkah-langkah	Pengguna

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	27

keselamatan siber dari diketahuimum. f. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada Pasukan CSIRT PKPP dengan segera; g. Menghadiri program-program kesedaran mengenai keselamatan siber ; dan h. Menandatangani surat akuan pematuhan Polisi Keselamatan Siber PKPP di Sistem Akuan PKS PKPP di https://akuanpks.pkpp.gov.my/ dan mencetak Surat Akuan yang dijana sebagaimana di Lampiran 1.	Pengguna
5.3 PENGASINGAN TUGAS (<i>SEGREGATION OF DUTIES</i>)	PERANAN
Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset. Perkara-perkara yang perlu dipatuhi adalah seperti yang 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 daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; c. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai <i>production</i>. 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;	Pengurus Bahagian/Ketua Unit

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	28

5.4 TANGGUNGJAWAB PENGURUSAN (MANAGEMENT RESPONSIBILITIES)	PERANAN
Pengurusan hendaklah memastikan warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.	Warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP.
5.5 HUBUNGAN DENGAN PIHAK BERKUASA (CONTACT WITH AUTHORITIES)	PERANAN
Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: - Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab PKPP; - Mewujud dan mengemas kini prosedur/senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia dan Suruhanjaya Komunikasi Dan Multimedia. Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba; dan - Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.	Pasukan CSIRT PKPP
5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS (CONTACT WITH SPECIAL INTEREST GROUPS)	PERANAN
Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau pun forum bagi: - meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat; - menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini; - berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan - berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	Warga PKPP (Mengikut Bidang Kepakaran)

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	29

5.7 RISIKAN ANCAMAN (<i>THREAT INTELLIGENCE</i>)	PERANAN
Risikan ancaman (<i>Threat Intelligence</i>) adalah serangkaian langkah dan tindakan yang diambil untuk mengesan, melindungi, dan mencegah berbagai jenis ancaman. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: - Sistem pemantauan keselamatan (<i>Security Monitoring</i>) bagi mengesan aktiviti yang mencurigakan atau ancaman perisian yang mungkin terjadi di dalam rangkaian atau sistem. - Memasang pendinding api (<i>Firewall</i>) bagi mengawal lalu lintas jaringan rangkaian daripada aktiviti yang mencurigakan. - Memastikan setiap perisian yang digunakan adalah yang terkini dan sentiasa dikemaskini. - Mengawal akses setiap pengguna aplikasi sistem mengikut skop tugas yang telah ditetapkan oleh pemilik sistem. - Mengkaji, menilai dan mengemaskini teknologi perkakasan atau perisian mengikut dengan keadaan semasa. - Risikan ancaman melibatkan pengumpulan, penilaian, analisis, dan pelaporan maklumat mengenai ancaman sedia ada atau baharu.	BTM
5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK (<i>INFORMATION SECURITY IN PROJECT MANAGEMENT</i>)	PERANAN
Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: - Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek di PKPP; - Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek; - Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenalpasti kawalan-kawalan yang diperlukan; dan - Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam polisi keselamatan siber PKPP.	Warga PKPP (Pasukan Projek)
5.9 INVENTORI MAKLUMAT DAN ASET YANG BERKAITAN	PERANAN

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	30

(INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS)	
1. Memastikan semua aset ICT PKPP hendaklah disokong dan diberi perlindungan yang bersesuaian. Perkara yang perlu dipatuhi adalah seperti berikut : a. Mengenal pasti Pegawai Penerima Aset setiap Bahagian untuk menguruskan penerimaan aset-aset ICT bagi projek-projek ICT; b. Memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumen, diselenggara dan dilupuskan. Maklumat aset direkodkan dan sentiasa dikemaskini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa; c. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja ; d. Pegawai Aset hendaklah mengesahkan penempatan aset ICT; e. Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, di dokumen dan dilaksanakan; dan f. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya. 2. Aset ICT yang di selenggara hendaklah milik PKPP. Perkara yang perlu dipatuhi oleh pemilik aset adalah seperti berikut: a. Memastikan aset ICT di bawah tanggungjawabnya telah dimasukkan dalam senarai aset; b. Memastikan aset ICT telah dikelaskan dan dilindungi; c. Mengenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan; d. Memastikan pengendalian aset ICT dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan e. Memastikan semua jenis aset dipelihara dengan baik.	Pegawai Penerima Aset, Pegawai Aset warga PKPP Pegawai Aset & warga PKPP
5.10 PENGGUNAAN MAKLUMAT DAN ASET BERKAITAN YANG BOLEH DITERIMA (ACCEPTABLE USE OF INFORMATION AND OTHER ASSOCIATED ASSETS)	PERANAN
Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.	Warga PKPP
5.11 PEMULANGAN ASET (RETURN OF ASSETS)	PERANAN
Memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak.	Warga PKPP

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	31

5.12 PENGELASAN MAKLUMAT (CLASSIFICATION OF INFORMATION)	PERANAN
Maklumat hendaklah dikelaskan sebagaimana yang ditetapkan di dalam Prosedur Kawalan Keselamatan Dokumen. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan seperti berikut: - Terkawal - Terbuka	Pegawai Integriti/Pengkelas
5.13 PELABELAN MAKLUMAT (LABELLING OF INFORMATION)	PERANAN
Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan.	Warga PKPP
5.14 PEMINDAHAN MAKLUMAT (INFORMATION TRANSFER)	PERANAN
- Perkara yang perlu dipatuhi adalah seperti yang berikut: - Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; - Terma pemindahan data, maklumat dan perisian antara PKPP dengan pihak luar hendaklah dimasukkan di dalam Perjanjian; - Media yang mengandungi maklumat perlu dilindungi; dan - Memastikan maklumat yang terdapat dalam mel elektronik hendaklah dilindungi sebaik-baiknya. - PKPP perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara PKPP dengan pihak luar. Perkara yang perlu dipatuhi adalah seperti yang berikut: - Pengurus Bahagian hendaklah mengawal penghantaran dan penerimaan maklumat PKPP; - Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat PKPP; - Mengenalpasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan - PKPP hendaklah mengenalpasti perlindungan	Pengguna, Warga PKPP dan pembekal ICTSO, Pengurus Bahagian

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	32

data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data. 3. Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Perkara yang perlu dipatuhi dalam pengendalian mel elektronik dan undang-undang bertulis lain yang berkuat kuasa adalah seperti: - Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”; - Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 — Pematuhan Tatacara Penggunaan E-mel dan Internet; - Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 - Langkah- langkah mengenai penggunaan Mel Elektronik Agensi-agensi Kerajaan; dan - mana-mana undang-undang bertulis Kerajaan Negeri yang berkuat kuasa;	Warga PKPP
4. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut : - Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh PKPP sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; - Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh PKPP; - Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; - Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; - Pengguna dinasihatkan menggunakan fail kepilkan, sekiranya perlu, tidak melebihi dua puluh lima megabait (25Mb) atau mengikut polisi yang ditetapkan agensi semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; - Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;	Warga PKPP

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	33

g. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; h. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; i. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; j. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; k. Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; l. Pengguna hendaklah memastikan alamat e-mel persendirian (seperti Yahoo Mail, Gmail, Hotmail dan sebagainya) tidak digunakan untuk tujuan rasmi; dan m. Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing.	Warga PKPP
5.15 KAWALAN AKSES (ACCESS CONTROL)	PERANAN
1. Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu diwujudkan, didokumenkan, dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini setahun sekali atau mengikut keperluan dan menyokong peraturan kawalan capaian sedia ada. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Keperluan keselamatan aplikasi; b. Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian; c. Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa; d. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; e. Pengasingan peranan kawalan capaian; f. Kebenaran rasmi permintaan akses; g. Keperluan semakan hak akses berkala;	Pemilik dan Pentadbir Sistem Aplikasi

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	34

h. Pembatalan hak akses; i. Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan j. Capaian <i>privilege</i>. 2. Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari PKPP. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Memastikan hanya pengguna yang dibenarkan sahaja boleh mendapat perkhidmatan rangkaian; b. Menempatkan, mengasingkan atau memasang peralatan ICT yang bersesuaian untuk kawalan keselamatan antara rangkaian PKPP, rangkaian agensi lain dan rangkaian awam; dan c. Mewujud, menguatkuasakan dan memantau mekanisme untuk pengesahan pengguna, ID pengguna, kata laluan atau peralatan ICT yang dihubungkan ke rangkaian termasuk rangkaian tanpa wayar; dan d. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pemilik dan Pentadbir Sistem Aplikasi
5.16 PENGURUSAN IDENTITI (IDENTITY MANAGEMENT)	PERANAN
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara-perkara berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh perbadanan sahaja boleh digunakan; b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c. Akaun pengguna yang diwujudkan pertama kali akan diberi capaian minimum yang akan ditetapkan oleh pemilik sistem; d. Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada pemilik perkhidmatan digital atau aplikasi terlebih dahulu; e. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan perbadanan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; f. Penggunaan akaun milik orang lain atau akaun yang dikongsi	Semua Pengguna dan Warga PKPP

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	35

bersama adalah dilarang; dan g. Pentadbir Sistem Aplikasi/Perkhidmatan Digital boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut : i) Pengguna bercuti panjang / menghadiri kursus di luar pejabat dalam tempoh waktu melebihi tiga (3) bulan; ii) Bertukar bidang tugas kerja; iii) Bertukar ke agensi lain; iv) Bersara; atau v) Ditamatkan perkhidmatan	Semua Pengguna dan Warga PKPP
5.17 MAKLUMAT PENGESAHAN (AUTHENTICATION INFORMATION)	PERANAN
Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.	ICTSO dan Pentadbir Perkhidmatan Aplikasi
5.18 HAK AKSES (ACCESS RIGHT)	PERANAN
1. Satu proses untuk penyediaan akses pengguna untuk kebenaran dan pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT. 2. Pemilik aset hendaklah menyemak hak akses pengguna pada sela masa yang ditetapkan. Pentadbir Perkhidmatan Aplikasi perlu mewujudkan Prosedur/SOP berkaitan Pendaftaran dan Penamatan Pengguna sistem masing-masing sebagai rujukan semakan ke atas hak akses pengguna pada sela masa yang ditetapkan. 3. Hak akses kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian atau diselaraskan apabila berlaku perubahan dalam jabatan.	ICTSO dan Pentadbir Perkhidmatan Aplikasi
5.19 KESELAMATAN MAKLUMAT DALAM HUBUNGAN PEMBEKAL (INFORMATION SECURITY IN SUPPLIER RELATIONSHIP)	PERANAN
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset PKPP. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Mengenalpasti dan mendokumentasi jenis pembekal mengikut kategori; b. Proses kitaran hayat (lifecycle) yang seragam untuk menguruskan pembekal; c. Mengawal dan memantau akses pembekal;	Pengurus Teknologi Maklumat, Pemilik Projek, Pembekal

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	36

d. Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian; e. Jenis-jenis obligasi kepada pembekal; f. Pelan kontigensi (<i>contingency plan</i>) bagi memastikan ketersediaan kemudahan pemprosesan maklumat; g. Melaksanakan program kesedaran terhadap Polisi Keselamatan Siber PKPP kepada pembekal; h. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber PKPP (Lampiran 3); dan i. Pembekal perlu mematuhi arahan keselamatan yang berkuatkuasa.	Pengurus Teknologi Maklumat, Pemilik Projek, Pembekal
5.20 MENANGANI KESELAMATAN MAKLUMAT DALAM PERJANJIAN PEMBEKAL (ADDRESSING INFORMATION SECURITY WITHIN SUPPLIER AGREEMENTS)	PERANAN
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. Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak PKPP selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa. Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak PKPP mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut: Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan; a. PKPP hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan; b. Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan; c. Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; d. Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian	Pembekal

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	37

teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal; e. Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut: • Badan penilai pihak ketiga adalah bebas dan berintegriti; • Badan penilai pihak ketiga adalah kompeten; • Kriteria penilaian; • Parameter pengujian; dan • Andaian yang di buat berkaitan dengan skop penilaian. f. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan PKPP; dan g. Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh PKPP.	Pembekal
5.21 PENGURUSAN KESELAMATAN MAKLUMAT DALAM RANTAIAN BEKALAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT) (MANAGING INFORMATION SECURITY IN THE INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SUPPLY CHAIN)	PERANAN
Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantai bekalan produk. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: a. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b. Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-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.	Pengurus Teknologi Maklumat, Pemilik Projek, Pembekal

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	38

5.22 PEMANTAUAN, SEMAKAN DAN PENGURUSAN PERUBAHAN PERKHIDMATAN PEMBEKAL (MONITORING, REVIEW AND CHANGE MANAGEMENT OF SUPPLIER SERVICES)	PERANAN
1. PKPP hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: - Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; - Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan - Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian. 2. Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahankan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan, dengan mengambil kira kepentingan maklumat, sistem dan proses perniagaan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti yang berikut: - Perubahan dalam perjanjian dengan pembekal; - Perubahan yang dilakukan oleh PKPP bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan - Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan subkontraktor.	Pengurus Teknologi Maklumat, Pemilik Projek, Pembekal
5.23 KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN AWAN (INFORMATION SECURITY FOR USE OF CLOUD SERVICES)	PERANAN
Perkhidmatan awan adalah penting untuk memastikan bahawa organisasi memilih penyedia perkhidmatan awan yang mempunyai tahap keselamatan yang tinggi. Berikut adalah beberapa langkah-langkah yang diperlukan sebelum penggunaan perkhidmatan awan. - Menetapkan skop perolehan perkhidmatan awan yang ingin dikawal. Skop ini perlu merangkumi jenis perkhidmatan awan yang diperlukan, data yang akan dipindahkan ke awan, dan syarat-syarat keselamatan yang dikehendaki. - Melakukan penilaian risiko untuk mengenal pasti potensi ancaman dan	ICTSO, Pentadbir Rangkaian

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	39

kerentanan yang berkaitan dengan penggunaan perkhidmatan awan. Ini memungkinkan anda untuk mengenal pasti tahap risiko dan mengambil tindakan untuk mengurangkan risiko tersebut. 3. Memilih penyedia perkhidmatan awan yang mematuhi piawaian keselamatan maklumat dan memiliki rekod prestasi yang baik dalam bidang keselamatan dan privasi data. 4. Membuat perjanjian perkhidmatan dengan penyedia perkhidmatan awan yang mencakupi butiran keselamatan maklumat, seperti tahap layanan, perlindungan data, pematuhan piawaian, pemisahan data, pemulihan bencana, dan pematuhan peraturan sebelum, semasa dan selepas tamat perjanjian perkhidmatan. 5. Melakukan audit keselamatan secara berkala ke atas penyedia perkhidmatan awan untuk memastikan pematuhan mereka terhadap perjanjian perkhidmatan dan piawaian keselamatan maklumat. 6. Memastikan bahawa penyedia perkhidmatan awan mempunyai perancangan pemulihan bencana yang kukuh untuk melindungi data organisasi dalam kejadian insiden yang merugikan. 7. Menilai semula keselamatan maklumat secara berkala dan memastikan ia selaras dengan keperluan keselamatan dan piawaian. 8. Memastikan bahawa organisasi mematuhi peraturan dan perundangan yang berkaitan dengan penggunaan perkhidmatan awan, terutamanya dalam hal privasi data dan perlindungan data peribadi.	ICTSO, Pentadbir Rangkaian
5.24 PERANCANGAN DAN PERSEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT (INFORMATION SECURITY INCIDENT MANAGEMENT PLANNING AND PREPARATION)	PERANAN
Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan tindak balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan insiden PKPP adalah berdasarkan kepada Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT PKPP yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Memberikan kesedaran berkaitan Prosedur Operasi Standard: Pengendalian Insiden Keselamatan ICT CSIRT PKPP dan hebahan kepada warga PKPP sekiranya ada perubahan; dan b. Memastikan pegawai yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.	Pengurus Teknologi Maklumat (ICTSO), CSIRT PKPP dan Pemilik Projek/Sistem Aplikasi

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	40

5.25 PENILAIAN DAN KEPUTUSAN TENTANG KEJADIAN KESELAMATAN MAKLUMAT (ASSESSMENT AND DECISION ON INFORMATION SECURITY EVENTS)	PERANAN
Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.	ICTSO
5.26 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT (RESPONSE TO INFORMATION SECURITY INCIDENT)	PERANAN
Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT PKPP. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut: - Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; - Menjalankan kajian forensik sekiranya perlu; - Menghubungi pihak yang berkenaan dengan secepat mungkin; - Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti; - Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; - Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; - Menyediakan tindakan pemulihan segera; dan - Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	ICTSO, CSIRT PKPP
5.27 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT (LEARNING FROM INFORMATION SECURITY INCIDENTS)	PERANAN
Pengetahuan yang diperoleh daripada penganalisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya. 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.	ICTSO, PKPP

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	41

5.28 PENGUMPULAN BUKTI (COLLECTION OF EVIDENCE)	PERANAN
PKPP hendaklah menentukan prosedur untuk mengenalpasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.	ICTSO, CSIRT PKPP
5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN (INFORMATION SECURITY DURING DISRUPTION)	PERANAN
1. PKPP hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, PKPP perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi PKPP. PKPP juga perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: - Melantik pasukan tadbir urus Pengurusan Kesenambungan Perkhidmatan (PKP) PKPP; - Menetapkan polisi PKP; - Mengenalpasti perkhidmatan kritikal; - Melaksanakan Kajian Impak Perkhidmatan (<i>Business Impact Analysis</i> — BIA) dan Penilaian Risiko terhadap perkhidmatan kritikal; - Membangunkan Pelan Induk Pengurusan Kesenambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT. - Melaksanakan program kesedaran dan latihan pasukan PKP dan warga PKPP; - Melaksanakan simulasi ke atas dokumen di para (c); dan - Melaksanakan penyelenggaraan ke atas pelan di para (c). 2. PKPP hendaklah menyediakan, mendokumenkan, melaksanakan dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:	Koordinator PKP, Disaster Recovery Team (DRT), Emergency Recovery Team (ERT), Critical Communication Team (CCT) PKPP Pengurusan Teraju, Koordinator PKP, Disaster Recovery Team (DRT),

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	42

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	43

2. Ini termasuk menentukan sumber daya ICT yang diperlukan, tujuan pemulihan, dan kebijakan perolehan peralatan dan perkhidmatan. 3. Mempunyai infrastruktur ICT yang <i>redundant</i>, termasuk rangkaian, pelayan, storan data, dan sokongan kuasa yang boleh berfungsi jika ada gangguan atau kegagalan. 4. Penggantian secara automatik (<i>failover</i>) dan peralatan cadangan perlu dipertimbangkan. 5. Lakukan pemantauan aktif terhadap peralatan ICT untuk mengenalpasti masalah sebelum ia berlaku dan mengelakkan gangguan. 6. Pengurusan inventori peralatan, pelan pembaikan, dan pemantauan prestasi berterusan. 7. Sediakan pelan pemulihan bencana ICT yang komprehensif. Ini termasuk cadangan data, pengekalkan cadangan pelayan, dan prosedur pemulihan semula aktiviti perniagaan. 8. Ujian dan latihan berkala pelan pemulihan bencana. 9. Pastikan akses kepada sistem dan data dikawal dengan ketat dan disemak secara berkala. Ini termasuk pengurusan identiti, pengesahihan dua faktor, dan peraturan akses yang ketat. 10. Sediakan perkhidmatan pengurusan keselamatan seperti antivirus, firewall, dan pelindung kegagalan untuk menghalang ancaman keselamatan ICT. 11. Amalkan pemantauan keselamatan untuk mengenalpasti dan tindak balas kepada ancaman dan insiden keselamatan. 12. Pastikan kakitangan tahu apa yang perlu dilakukan dalam kes insiden keselamatan. 13. Melaksanakan penyelenggaraan dan pembaikan peralatan dan sistem secara berkala untuk mengelakkan kegagalan yang tidak dijangka. 14. Tetapkan jadual pembaikan berkala dan pemulihan data. 15. Pantau penggunaan sumber daya ICT seperti bandwidth dan kapasiti penyimpanan untuk mengelakkan penggunaan berlebihan yang boleh menyebabkan gangguan. 16. Pastikan penyedia perkhidmatan awan atau penyedia perkhidmatan lain mempunyai pelan kesinambungan perniagaan yang mencukupi yang dapat menyokong operasi jika berlaku gangguan.	Pengurus Teknologi Maklumat, ICTSO, Pentadbir Rangkaian, Pentadbir Sistem Aplikasi
---	---

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	44

5.31 KEPERLUAN UNDANG-UNDANG, BERKANUN, PERATURAN DAN KONTRAK (LEGAL, STATUTORY, REGULATORY AND CONTRACTUAL REQUIREMENTS)	PERANAN
Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP. Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di PKPP dan pembekal adalah seperti di Lampiran 2.	Warga PKPP, pembekal, pakar runding daripada pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP
5.32 HAK HARTA INTELEK (INTELLECTUAL PROPERTY RIGHTS)	PERANAN
Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan pelesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	Warga PKPP, pembekal, pakar runding daripada pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP
5.33 PERLINDUNGAN REKOD (PROTECTION OF RECORDS)	PERANAN
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.	Warga PKPP, pembekal, pakar runding daripada pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP
5.34 KERAHSIAAN DAN PERLINDUNGAN MAKLUMAT PENGENALAN PERIBADI (PRIVACY AND PROTECTION OF PERSONAL IDENTIFIABLE INFORMATION (PII))	PERANAN
PKPP hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.	Warga PKPP, pembekal, pakar runding daripada pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP
5.35 PENILAIAN KESELAMATAN MAKLUMAT OLEH PIHAK BERKECUALI (INDEPENDENT REVIEW OF INFORMATION SECURITY)	PERANAN
Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	Pengurus Teknologi Maklumat dan Pemilik Perkhidmatan Digital

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	45

5.36 PEMATUHAN POLISI, PERATURAN DAN PIAWAIAN KESELAMATAN MAKLUMAT (COMPLIANCE WITH POLICIES, RULES AND STANDARD FOR INFORMATION SECURITY)	PERANAN
1. PKPP hendaklah membuat kajian semula secara berkala terhadap pematuhan dasar dan standard keselamatan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan polisi, piawaian dan keperluan teknikal yang bersesuaian. 2. PKPP hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung di dalam polisi, piawaian dan keperluan komputer.	Pengurus Teknologi Maklumat dan Pemilik Perkhidmatan Digital
5.37 PROSEDUR OPERASI YANG DIDOKUMENKAN (DOCUMENTED OPERATING PROCEDURE)	PERANAN
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Semua prosedur keselamatan siber yang diwujudkan, dikenal pasti dan masih diguna pakai hendaklah didokumen, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian serta pemprosesan maklumat, pengendalian serta penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	BTM, CSIRT PKPP

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	46

6.0 KAWALAN MANUSIA (PEOPLE CONTROL)	
6.1 SARINGAN (SCREENING)	PERANAN
Tapisan keselamatan hendaklah dijalankan terhadap warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: - Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan - Menjalankan tapisan keselamatan untuk PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP
6.2 TERMA DAN SYARAT PERJAWATAN (TERMS AND CONDITION EMPLOYMENT)	PERANAN
Persetujuan berkontrak dengan warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara- perkara yang mesti dipatuhi adalah seperti yang berikut: - Menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP yang terlibat dalam menjamin keselamatan aset ICT; dan - Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	47

6.3 KESEDARAN, PENDIDIKAN DAN LATIHAN KESELAMATAN MAKLUMAT (INFORMATION SECURITY AWARENESS AND TRAINING)	PERANAN
Warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP 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 yang berikut : - memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber PKPP, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka; - memastikan kesedaran yang berkaitan Polisi Keselamatan Siber PKPP perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan - memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.	Warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP
6.4 PROSES TATATERTIB (DISCIPLINARY PROCESS)	PERANAN
Proses tatatertib yang formal dan disampaikan kepada warga PKPP hendaklah tersedia bagi membolehkan tindakan diambil terhadap warga PKPP yang melakukan pelanggaran keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: - Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga PKPP sekiranya berlaku pelanggaran terhadap perundangan dan peraturan yang ditetapkan oleh PKPP; - Warga PKPP yang melanggar polisi ini akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT PKPP.	Unit Integriti

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	48

6.5 TANGGUNGJAWAB SELEPAS PENAMATAN ATAU PERTUKARAN PERJAWATAN (<i>RESPONSIBILITIES AFTER TERMINATION OR CHANGE OF EMPLOYMENT</i>)	PERANAN
Warga PKPP yang telah tamat perkhidmatan/bertukar perkhidmatan perlu mematuhi perkara-perkara berikut: - Memastikan semua aset ICT PKPP dikembalikan kepada PKPP mengikut peraturan dan/atau terma yang ditetapkan; - Memastikan semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat dibatalkan oleh pentadbir sistem mengikut peraturan yang ditetapkan oleh PKPP; - Maklumat rasmi PKPP dalam peranti tidak dibenarkan dibawa keluar dari PKPP; - Menyedia dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan. Bahagian Pengurusan Sumber Manusia perlu: - Mengemaskini semua dokumentasi berkaitan pegawai yang tamat perkhidmatan bagi memastikan kesinambungan perkhidmatan PKPP.	Warga PKPP
6.6 PERJANJIAN KERAHSIAAN (<i>CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS</i>)	PERANAN
Syarat-syarat perjanjian kerahsiaan atau <i>non-disclosure</i> perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : - Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pembekal; - Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak pembekal perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan - Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	ICTSO, Pentadbir Sistem Aplikasi, Pengguna dan Pembekal

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	49

6.7 TELEKERJA (<i>REMOTE WORKING</i>)	PERANAN
a. Capaian jarak jauh yang dimaksudkan merangkumi: i. capaian daripada sistem rangkaian dalaman; dan ii. capaian daripada sistem rangkaian luaran bagi lokasi luar pejabat untuk tujuan <i>teleworking</i>. b. Penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi (<i>encryption</i>); c. Lokasi bagi akses ke sistem aplikasi PKPP hendaklah dipastikan selamat; d. Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pentadbir Rangkaian dan Keselamatan. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini; dan e. Capaian jarak jauh hendaklah menggunakan kemudahan yang disediakan oleh jabatan.	ICTSO, Pentadbir Rangkaian
6.8 PELAPORAN KEJADIAN KESELAMATAN MAKLUMAT (<i>INFORMATION SECURITY EVENT REPORTING</i>)	PERANAN
1. Insiden keselamatan maklumat seperti berikut hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada CSIRT PKPP kemudiannya perlu melaporkan kepada ICTSO dengan kadar segera. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Maklumat didapati atau disyaki hilang, atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses didapati atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e. Berlaku percubaan mencerooboh, penyelewengan dan insiden-insiden yang tidak dijangka. Prosedur pelaporan insiden keselamatan Siber berdasarkan: a. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan	Warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	50

Insiden Keselamatan Teknologi Maklumat dan Komunikasi; b. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam; c. Surat Arahan CIO 18 Februari 2011 – Proses Kerja Pelaporan Insiden Keselamatan ICT <i>Computer Emergency Response Team</i> (CSIRT) PKPP; d. Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT PKPP; dan e. Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan Dan Pengendalian Insiden Keselamatan Siber Sektor Awam. f. Akta Keselamatan Siber 2024 dan Peraturan-peraturan [Akta 854] 2. Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika perlu dikelaskan sebagai insiden keselamatan maklumat.	ICTSO
--	-------

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	51

7.0 KAWALAN FIZIKAL (PHYSICAL CONTROL)	
7.1 PERIMETER KESELAMATAN FIZIKAL (PHYSICAL SECURITY PERIMETERS)	PERANAN
Ini bertujuan untuk menghalang akses tanpa kebenaran serta kerosakan dan gangguan secara fizikal terhadap premis, maklumat dan Aset ICT PKPP. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: - Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; - Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; - Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; - Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan manusia; - Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; - Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan - Memasang alat penggera atau kamera keselamatan;	BPSM
7.2 KEMASUKAN FIZIKAL (PHYSICAL ENTRY)	PERANAN
1. Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis PKPP. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: - Setiap warga PKPP hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas; - Semua pas keselamatan hendaklah diserahkan kembali kepada jabatan apabila pengguna bertukar, tamat perkhidmatan atau bersara; - Setiap pelawat boleh mendapatkan Pas Keselamatan Pelawat di Lobi Kaunter Perkhidmatan PKPP terlebih dahulu	Warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	52

dan hendaklah dikembalikan semula selepas tamat lawatan; d. Kehilangan pas mestilah dilaporkan dengan segera; dan e. Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan Aset ICT PKPP. 2. Titik kemasukan (<i>access point</i>) seperti kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan. 3. PKPP hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.	BPSM
7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN (<i>SECURING OFFICES, ROOMS AND FACILITIES</i>)	PERANAN
Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Kawasan tempat bekerja, bilik mesyuarat, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan 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.	Warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP
7.4 PEMANTAUAN KESELAMATAN FIZIKAL (<i>PHYSICAL SECURITY MONITORING</i>)	PERANAN
Akses tanpa kebenaran ke kawasan fizikal terhad seperti bilik pelayan dan bilik peralatan IT boleh mengakibatkan kehilangan kerahsiaan, ketersediaan, integriti dan keselamatan aset maklumat. Berikut adalah kawalan yang boleh dilaksanakan: a. Kamera CCTV b. Pengawal keselamatan c. Penggera keselamatan untuk penceroboh d. Alat perisian untuk pengurusan keselamatan fizikal	Pentadbir Pusat Data dan BPSM
7.5 PERLINDUNGAN DARI ANCAMAN FIZIKAL DAN PERSEKITARAN (<i>PROTECTION AGAINST PHYSICAL AND ENVIRONMENTAL THREATS</i>)	PERANAN
Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. PKPP	Pentadbir Pusat Data dan BPSM

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	53

perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.	
7.6 BEKERJA DI KAWASAN YANG SELAMAT (<i>WORKING INSECURE AREA</i>)	PERANAN
Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga PKPP yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis PKPP termasuklah Pusat Data. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas kawasan tersebut adalah seperti yang berikut: - Sumber data atau server, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran; - Akses adalah terhad kepada warga PKPP yang telah diberi kuasa sahaja dan dipantau pada setiap masa; - Pemantauan dibuat menggunakan <i>Closed-Circuit Television</i> (CCTV) kamera atau lain-lain peralatan yang sesuai; - Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual; - Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; - Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; - Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggaran, saliran air dan laluan awam; - Memperkuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; - Memperkuhkan dinding dan siling; dan - Mengehadkan jalan keluar masuk.	Pentadbir Pusat Data dan BPSM
7.7 MEJA KOSONG DAN SKRIN KOSONG (<i>CLEAR DESK AND CLEAR SCREEN</i>)	PERANAN
Dasar meja kosong untuk kertas dan media penyimpanan boleh alih serta dasar skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan. Semua maklumat dalam apa jua bentuk media hendaklah	Warga PKPP, pembekal, pakar runding dan pihak yang

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	54

disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. <i>Clear Desk</i> dan <i>Clear Screen</i> bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : - Menggunakan kemudahan <i>screen saver password</i> atau <i>logout</i> apabila meninggalkan komputer; - Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan - Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat. - E-mel masuk dan keluar hendaklah dikawal; dan - Menghalang penggunaan tanpa kebenaran bagi peralatan seperti mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.	mempunyai urusan dengan perkhidmatan ICT PKPP
7.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN (<i>EQUIPMENT SITING AND PROTECTION</i>)	PERANAN
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: - Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; - Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; - Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; - Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pegawai Aset ICT; - Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; - Pengguna mesti memastikan perisian <i>antivirus</i> di komputer peribadi mereka sentiasa aktif (<i>activated</i>) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;	Warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	55

- g. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;
- h. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;
- i. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set (Gen-Set)*;
- j. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *router* dan lain-lain perlu diletakkan di dalam rak khas;
- k. Semua peralatan yang digunakan secara berterusan tanpa henti mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;
- l. Peralatan ICT yang hendak dibawa keluar dari premis jabatan perlu mendapat kelulusan Pegawai Aset ICT dan direkodkan bagi tujuan pemantauan;
- m. Peralatan ICT yang hilang hendaklah dilaporkan kepada Pegawai Aset ICT dengan segera;
- n. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;
- o. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset ICT;
- p. Sebarang kerosakan peralatan ICT hendaklah dilaporkan melalui Sistem Aduan melalui Portal PKPP untuk dibaik pulih;
- q. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan pada semua Aset ICT. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;
- r. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;
- s. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;
- t. Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "OFF" apabila meninggalkan pejabat;

Warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT
PKPP

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	56

u. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada Pengurus Bahagian Teknologi Maklumat; dan v. Memastikan plag dicabut daripada suis utama (<i>main switch</i>) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya. w. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi sahaja.	Warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP
7.9 KESELAMATAN ASET DI LUAR PREMIS (<i>SECURITY OF ASSETS OF PREMISES</i>)	PERANAN
Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis PKPP. Peralatan yang dibawa keluar dari premis PKPP adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Peminjam perlu bertanggungjawab terhadap keselamatan Aset ICT yang dipinjam; b. Aset ICT perlu dilindungi dan dikawal sepanjang masa; c. Penyimpanan atau penempatan Aset ICT perlu mengambil kira ciri-ciri keselamatan lokasi yang bersesuaian; dan d. Sebarang kehilangan semasa peminjaman Aset ICT tersebut perlulah dilaporkan kepada pihak Berkuasa dan kepada Pegawai Aset ICT.	Warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP
7.10 MEDIA STORAN (<i>STORAGE MEDIA</i>)	PERANAN
1. Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh PKPP. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut: a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d. Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan	Pentadbir Sistem Aplikasi dan Pengguna

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	57

e. Menyimpan semua jenis media di tempat yang selamat. 2. Prosedur pelupusan media adalah seperti berikut: a. Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh PKPP. b. Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa. 3. Prosedur pemindahan media fizikal adalah seperti berikut: a. Pemindahan media fizikal keluar premis perlu mendapat kelulusan dan mengikut kaedah pemindahan aset ICT yang ditetapkan oleh PKPP. b. Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dipindahkan mengikut prosedur yang berkuat kuasa. 4. Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Aset ICT yang dibawa untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan Aset ICT: a. Aset ICT yang dibawa keluar dari premis PKPP mestilah mendapat kelulusan Pegawai Aset ICT atau Ketua Bahagian/Unit atau Pengurus ICT dan tertakluk kepada tujuan yang dibenarkan; b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan;	Pentadbir Sistem Aplikasi dan Jawatankuasa yang dilantik untuk pelupusan aset. Pemilik media Pengguna, Pegawai Aset
7.11 UTILITI SOKONGAN (SUPPORTING UTILITIES)	PERANAN
Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Semua alat sokongan perlu diselenggara dari semasa ke semasa (sekurang-kurangnya setahun sekali).	Warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	58

7.12 KESELAMATAN KABEL (<i>CABLING SECURITY</i>)	PERANAN
Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah- langkah keselamatan yang perlu diambil adalah seperti yang berikut: - Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; - Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; - Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan <i>wire tapping</i>, dan - Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui <i>trunking</i> bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	BTM, BPSM
7.13 PENYELENGGARAAN PERKAKASAN (<i>EQUIPMENT MAINTENANCE</i>)	PERANAN
Peralatan ICT hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti yang berterusan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: - Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi yang telah ditetapkan oleh pengeluar; - Memastikan perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; - Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; - Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; - Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan - Semua penyelenggaraan mestilah mendapat kebenaran daripada Pegawai Aset ICT.	Pentadbir Teknikal

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	59

7.14 PELUPUSAN SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN (<i>SECURE DISPOSAL OR RE-USE OF EQUIPMENT</i>)	PERANAN
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh PKPP dan ditempatkan di bahagian/unit atau Jabatan Kerajaan Negeri. Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (<i>overwrite</i>) sebelum dilupuskan atau diguna semula. Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh PKPP dan ditempatkan di PKPP. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan di PKPP. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: - Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu dengan cara yang selamat; - Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; - Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; - Pegawai Aset ICT hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; - Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; - Pegawai Aset ICT bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset; - Pelupusan peralatan ICT PKPP hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan - Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut:	Pegawai Aset ICT dan Warga PKPP

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	60

1. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, hardisk, motherboard dan sebagainya; 2. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke lokasi berlainan tanpa kebenaran; 3. Memindah keluar dari Agensi atau Jabatan bagi mana-mana peralatan ICT milik PKPP yang hendak dilupuskan tanpa kebenaran; 4. Melupuskan sendiri peralatan ICT PKPP kerana kerja-kerja pelupusan di bawah tanggungjawab PKPP; dan 5. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti thumb drive atau external hard disk sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	Pegawai Aset ICT dan Warga PKPP
---	------------------------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	61

8 KAWALAN TEKNOLOGI (TECHNOLOGICAL CONTROL)	
8.1 PERANTI PENGGUNA (USER END POINT DEVICES)	PERANAN
1. Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut: - Tamatkan sesi aktif apabila selesai tugas; <i>Log-off</i> komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan - Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan. 2. Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: - Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek di PKPP; - Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek; - Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenalpasti kawalan-kawalan yang diperlukan; dan - Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam polisi keselamatan siber PKPP	Warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP
8.2 HAK AKSES ISTIMEWA (PRIVILEGED ACCESS RIGHT)	PERANAN
Hak akses istimewa membolehkan PKPP mengawal akses kepada infrastruktur, aplikasi, aset PKPP dan mengekalkan integriti semua data dan sistem yang disimpan. PKPP hendaklah: - Kenal pasti senarai pengguna yang memerlukan sebarang tahap akses istimewa – sama ada untuk sistem individu – seperti pangkalan data – aplikasi atau OS asas. - Kekalkan dasar yang memperuntukkan hak akses istimewa	Pengguna, Pentadbir Perkhidmatan Aplikasi, ICTSO

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	62

kepada pengguna pada apa yang dikenali sebagai "acara mengikut acara asas" - pengguna harus diberikan tahap akses berdasarkan minimum yang diperlukan untuk mereka menjalankan peranan mereka. c. Menggariskan proses kebenaran yang jelas yang berurusan dengan semua permintaan untuk akses istimewa, termasuk menyimpan rekod semua hak akses yang telah dilaksanakan. d. Pastikan hak akses tertakluk pada tarikh luput yang berkaitan. e. Ambil langkah untuk memastikan bahawa pengguna mengetahui dengan jelas sebarang tempoh masa di mana mereka beroperasi dengan akses istimewa kepada sistem. f. Jika berkaitan, pengguna diminta untuk mengesahkan semula sebelum menggunakan hak akses istimewa, untuk menjejaskan keselamatan maklumat/data yang lebih besar. g. Menjalankan audit berkala ke atas hak akses istimewa, terutamanya selepas tempoh perubahan jabatan. Hak akses pengguna harus disemak berdasarkan "tugas, peranan, tanggungjawab dan kecekapan" mereka. h. Pertimbangkan untuk beroperasi dengan memastikan hak akses istimewa diberikan dalam tettingkap masa yang dikawal ketat yang memenuhi keperluan minimum untuk operasi yang akan dijalankan (perubahan kritikal, pentadbiran sistem dsb). i. Pastikan semua aktiviti akses istimewa dicatatkan dengan sewajarnya. j. Cegah penggunaan maklumat log masuk sistem generik (terutamanya nama pengguna dan kata laluan piawai). k. Mematuhi dasar memberikan pengguna dengan identiti yang berasingan, yang membolehkan kawalan yang lebih ketat ke atas hak akses istimewa. Identiti sedemikian kemudiannya boleh dikumpulkan bersama, dengan kumpulan yang berkaitan diberikan tahap hak akses yang berbeza. l. Pastikan hak akses istimewa dikhaskan untuk tugas kritikal sahaja, yang berkaitan dengan operasi berterusan rangkaian ICT yang berfungsi – seperti pentadbiran sistem dan penyelenggaraan rangkaian.	Pengguna, Pentadbir Perkhidmatan Aplikasi, ICTSO
--	---

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	63

8.3 SEKATAN AKSES MAKLUMAT (<i>INFORMATION ACCESS RESTRICTION</i>)	PERANAN
Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian.	Pegguna, Pentadbir Perkhidmatan Aplikasi, ICTSO
8.4 AKSES KEPADA KOD SUMBER (<i>ACCESS TO SOURCE CODE</i>)	PERANAN
Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut: - Log audit perlu dikekalkan kepada semua akses kepada kod sumber; - Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan - Kod sumber (<i>source code</i>) bagi semua aplikasi dan perisian adalah menjadi hak milik PKPP.	Pengarah Projek, Pengurus Projek dan Pentadbir Perkhidmatan Digital
8.5 PENGESAHAN KESELAMATAN (<i>SECURE AUTHENTICATION</i>)	PERANAN
Kawalan capaian terhadap sistem aplikasi perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan adalah seperti yang berikut: - Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan; - Menjana amaran (<i>alert</i>) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem; - Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin; - Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna; - Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : - Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; - Pegguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; - Panjang kata laluan mestilah sekurang-kurangnya DUA	Pentadbir Perkhidmatan Digital, ICTSO

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	64

BELAS (12) AKSARA dengan gabungan antara huruf, aksara khas dan nombor (alphanumeric) KECUALI bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad; iv. Kata laluan tidak boleh didedahkan dengan apa cara sekalipun; v. Kata laluan papan kekunci (lock screen) dan screen saver hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; vi. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara; vii. Bagi sistem aplikasi, kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula; viii. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; ix. Bagi sistem aplikasi, had cubaan kemasukan kata laluan bagi capaian adalah maksimum tiga (3) kali sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan dibekukan. Kemasukan kata laluan seterusnya hanya boleh dibuat selepas bagi tempoh masa tertentu (mengikut kesesuaian sistem) atau setelah diset semula oleh Pentadbir Sistem Aplikasi/Perkhidmatan Digital; x. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; xi. Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna. f. Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	Pentadbir Perkhidmatan Digital, ICTSO
8.6 PENGURUSAN KAPASITI (CAPACITY MANAGEMENT)	PERANAN
Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. Perkara-perkara yang perlu dipatuhi adalah seperti berikut :	Pemilik Sistem Aplikasi, Pentadbir Sistem Aplikasi

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	65

a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan b. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pemilik Sistem Aplikasi, Pentadbir Sistem Aplikasi
8.7 PERLINDUNGAN DARIPADA PERISIAN HASAD (<i>PROTECTION AGAINST MALWARE</i>)	PERANAN
Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan malware hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya adalah seperti berikut : - Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti Antivirus, <i>Intrusion Detection System</i> (IDS) dan <i>Intrusion Prevention System</i> (IPS), <i>Content filtering</i> dan <i>Web Application Firewall</i> (WAF) serta mengikut prosedur penggunaan yang betul dan selamat; - Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; - Memastikan perisian antivirus mempunyai pengurusan berpusat bagi memudahkan penetapan polisi dan penyediaan laporan jika berlaku <i>virus outbreak</i> dalam rangkaian; - Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya serta dilaksanakan secara berkala; dan - Mengemas kini antivirus dengan signature/<i>pattern</i> terkini.	Pentadbir Teknikal, Pentadbir Rangkaian, Pengguna
8.8 PENGURUSAN KERENTANAN TEKNIKAL (<i>MANAGEMENT OF TECHNICAL VULNERABILITIES</i>)	PERANAN
1. Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan jabatan terhadap kerentanan tersebut hendaklah dinilai dan langkah- langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan.	Pentadbir Sistem Aplikasi dan Pasukan CSIRT PKPP

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	66

Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem aplikasi dan operasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: - Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi; - Menganalisis tahap risiko kerentanan; dan - Mengambil tindakan pengolahan dan kawalan risiko. 2. PKPP hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung dalam polisi, piawaian dan keperluan komputer.	Pengurus ICT dan Pemilik Perkhidmatan Digital
8.9 PENGURUSAN KONFIGURASI (CONFIGURATION MANAGEMENT)	PERANAN
Pengurusan konfigurasi ialah bahagian penting dalam operasi pengurusan aset organisasi yang lebih luas. Konfigurasi adalah kunci dalam memastikan rangkaian bukan sahaja beroperasi sebagaimana mestinya, tetapi juga dalam melindungi peranti daripada perubahan yang tidak dibenarkan atau pindaan yang salah di pihak kakitangan penyelenggaraan dan/atau vendor. Perkara yang perlu dipatuhi adalah seperti yang berikut: - Cuba untuk menggunakan panduan khusus vendor dan/atau sumber terbuka yang tersedia secara umum tentang cara terbaik untuk mengkonfigurasi aset perkakasan dan perisian. - Memenuhi keperluan keselamatan minimum untuk peranti, aplikasi atau sistem yang sesuai untuknya. - Bekerja selaras dengan usaha keselamatan maklumat organisasi yang lebih luas, termasuk semua kawalan ISO yang berkaitan. - Perlu diingat keperluan perniagaan unik PKPP- terutamanya dalam hal konfigurasi keselamatan - termasuk kebolehlaksanaan untuk menggunakan atau mengurus templat pada bila-bila masa. - Disemak pada selang masa yang sesuai untuk memenuhi kemas kini sistem dan/atau perkakasan, atau sebarang ancaman keselamatan yang berlaku.	ICTSO dan Pentadbir Sistem Aplikasi
8.10 PENGHAPUSAN MAKLUMAT (INFORMATION DELETION)	PERANAN
Organisasi harus sedar tentang kewajipan mereka untuk memadamkan data yang disimpan pada <i>server</i>, <i>hard disk</i>, <i>data array</i> dan <i>USB</i> apabila ia tidak lagi diperlukan dengan:	ICTSO dan Pentadbir Sistem Aplikasi

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	67

a. Pilih kaedah pemadaman yang sesuai yang mematuhi mana-mana undang-undang atau peraturan sedia ada. Pilihan termasuk pemadaman biasa, tulis ganti atau penghapusan dikodkan. Pastikan bahawa, apabila menggunakan vendor pemadaman khusus, organisasi memperoleh bukti yang mencukupi (biasanya melalui dokumentasi) bahawa pemadaman telah dilakukan. b. Organisasi harus menyatakan dengan tepat keperluan mereka apabila menggunakan vendor pihak ketiga, termasuk kaedah pemadaman dan jangka masa, dan harus menjamin bahawa aktiviti pemadaman dimasukkan dalam kontrak yang mengikat.	ICTSO dan Pentadbir Sistem Aplikasi
8.11 PELITUPAN DATA (DATA MASKING)	PERANAN
Apabila menggunakan salah satu daripada teknik ini, organisasi harus mempertimbangkan: a. Tahap pelitupan dan/atau penyamaran yang diperlukan, berbanding dengan sifat data. b. Cara <i>data masking</i> sedang diakses. c. Sebarang perjanjian mengikat yang menyekat penggunaan data untuk disembunyikan. d. Mengekalkan <i>data masking</i> berasingan daripada mana-mana jenis data lain, untuk mengelakkan subjek data dikenal pasti dengan mudah. e. Meneliti data yang diterima, dan bagaimana ia telah diberikan kepada mana-mana sumber dalaman atau luaran.	ICTSO dan Pentadbir Sistem Aplikasi
8.12 PENCEGAHAN KEBOCORAN DATA (DATA LEAKAGE PREVENTION)	PERANAN
Kebocoran data sukar untuk dihapuskan sepenuhnya. Walau bagaimanapun, untuk meminimumkan risiko yang unik untuk operasi perkhidmatan, jabatan harus: a. Klasifikasikan data selaras dengan piawaian industri yang diiktiraf (PII, data komersial, maklumat produk), untuk menetapkan tahap risiko yang berbeza-beza di seluruh bahagian. b. Memantau dengan teliti saluran data yang diketahui yang banyak digunakan dan terdedah kepada kebocoran (cth. e-mel, pemindahan fail dalaman dan luaran, peranti USB).	ICTSO, Pentadbir Sistem Aplikasi, Pentadbir Rangkaian

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	68

c. Hadkan keupayaan pengguna untuk menyalin dan menampal data (jika berkenaan) ke dan dari platform dan sistem tertentu. d. Kebenaran daripada pemilik data sebelum sebarang pemindahan data dilaksanakan. e. Pertimbangkan untuk mengurus atau menghalang pengguna daripada mengambil tangkapan skrin atau mengambil gambar monitor yang memaparkan jenis data yang dilindungi. f. Sulitkan sandaran yang mengandungi maklumat sensitif. g. Merangka langkah keselamatan pintu masuk dan langkah pencegahan kebocoran yang melindungi daripada faktor luaran seperti (tetapi tidak terhad kepada) pengintipan industri, sabotaj, gangguan komersial dan/atau kecurian IP. h. Memastikan perisian operating sistem dan antivirus sentiasa dikemaskini.	ICTSO, Pentadbir Sistem Aplikasi, Pentadbir Rangkaian
8.13 SANDARAN MAKLUMAT (INFORMATION BACKUP)	PERANAN
Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, <i>backup</i> hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Membuat <i>backup</i> keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat <i>backup</i> ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan <i>backup</i> bergantung pada tahap kritikal maklumat; c. Menguji sistem <i>backup</i> dan prosedur <i>restore</i> sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana. d. Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara <u>harian</u>, <u>mingguan</u>, <u>bulanan</u> atau <u>tahunan</u>. Kekerapan sandaran bergantung pada tahap kritikal maklumat, dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi <i>backup</i>; dan e. Merekod dan menyimpan salinan <i>backup</i> di lokasi yang berlainan (<i>off-site</i>) dan selamat.	Pentadbir Sistem Aplikasi, Pentadbir Pusat Data

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	69

8.14 KETERSEDIAAN KEMUDAHAN PEMROSESAN MAKLUMAT (REDUNDANCY OF INFORMATION PROCESSING FACILITIES)	PERANAN
Kemudahan pemprosesan maklumat PKPP perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji (<i>failover test</i>) keberkesanannya dari semasa ke semasa.	Pentadbir Pusat Data, Pemilik Perkhidmatan Digital dan Pentadbir Sistem Aplikasi
8.15 LOGGING (LOGGING)	PERANAN
1. Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan. Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data. Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti berikut : - fail log sistem pengoperasian; - fail log servis (web, e-mel); - fail log aplikasi (<i>audit trail</i>); dan - fail log rangkaian (<i>switch, firewall, IPS</i>) Pentadbir Sistem Aplikasi/Perkhidmatan Digital hendaklah melaksanakan perkara-perkara berikut : - Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; - Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan - Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada CSIRT PKPP. 2. Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan capaian tanpa izin. 3. Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula	Pentadbir Sistem Aplikasi Pentadbir Sistem Aplikasi Pentadbir Sistem Aplikasi dan Pasukan CSIRT PKPP

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	70

secara tetap. - Memantau penggunaan kemudahan memproses maklumat secara berkala; - Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke semasa dan menyediakan laporan jika perlu; - Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; - Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; - Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada Pasukan CSIRT PKPP.	Pentadbir Sistem Aplikasi dan Pasukan CSIRT PKPP
8.16 AKTIVITI PEMANTAUAN (MONITORING ACTIVITIES)	PERANAN
PKPP hendaklah memasukkan perkara berikut dalam operasi pemantauan jabatan: - Kedua-dua trafik rangkaian masuk dan keluar, termasuk data ke dan dari aplikasi; - Akses kepada platform kritikal organisasi, termasuk (tetapi tidak terhad kepada Sistem, Pelayan, Perkakasan rangkaian); - Sistem pemantauan itu sendiri; - Fail konfigurasi; - Log peristiwa daripada peralatan keselamatan dan platform perisian; - Semakan kod yang memastikan mana-mana program boleh digunakan adalah dibenarkan dan bebas daripada ancaman; - Pengiraan, penyimpanan dan penggunaan sumber rangkaian.	ICTSO, Pentadbir Rangkaian
8.17 PENYEGERAKAN JAM (CLOCK SYNCHRONISATION)	PERANAN
Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain PKPP atau domain keselamatan hendaklah disegerakkan mengikut sumber rujukan masa tunggal.	Pentadbir Pusat Data, Pentadbir Rangkaian, Pentadbir Teknikal

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	71

Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam PKPP atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh <i>National Metrology Institute of Malaysia</i> (NMIM).	Pentadbir Pusat Data, Pentadbir Rangkaian, Pentadbir Teknikal
8.18 PENGGUNAAN UTILITI PROGRAM ISTIMEWA (USE OF PRIVILEGED UTILITY PROGRAMS)	PERANAN
Untuk mengekalkan integriti rangkaian dan meningkatkan kesinambungan perniagaan, PKPP hendaklah: - Hadkan penggunaan program utiliti kepada pekerja dan kakitangan penyelenggaraan IT yang secara khusus memerlukan mereka menjalankan peranan kerja mereka. - Pastikan semua program utiliti dikenal pasti, disahkan dan dibenarkan selaras dengan keperluan perniagaan, dan pihak pengurusan dapat memperoleh pandangan atas bawah penggunaannya pada bila-bila masa. - Kenal pasti semua kakitangan yang menggunakan program utiliti, sama ada sebagai sebahagian daripada tugas harian mereka, atau secara ad-hoc. - Laksanakan kawalan kebenaran yang mencukupi untuk mana-mana pekerja yang perlu menggunakan program utiliti, sama ada sebagai sebahagian daripada tugas harian mereka atau secara ad-hoc. - Menghalang penggunaan program utiliti pada mana-mana sistem yang dianggap perlu oleh organisasi untuk mengasingkan tugas. - Semak semula penggunaan program utiliti secara berkala dan sama ada alih keluar atau lumpuhkan sebarang program seperti yang diperlukan oleh organisasi. - Program utiliti partition berbeza daripada aplikasi standard yang digunakan oleh perniagaan secara tetap, termasuk trafik rangkaian. - Hadkan ketersediaan program utiliti, dan gunakannya untuk tujuan nyata sahaja. - Log penggunaan program utiliti, termasuk cap masa dan pengguna yang dibenarkan.	ICTSO, Pentadbir Teknikal, Pentadbir Rangkaian

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	72

8.19 PEMASANGAN PERISIAN PADA SISTEM OPERASI (INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS)	PERANAN
1. Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti yang berikut: a. Strategi <i>rollback</i> perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian; b. Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; dan c. Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur. 2. Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP. b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; dan c. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.	Pentadbir Sistem Aplikasi Pentadbir SistemAplikasi, Warga PKPP, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT PKPP
8.20 KESELAMATAN RANGKAIAN (NETWORKS SECURITY)	PERANAN
Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. Semua peralatan mestilah melalui proses <i>Factory Acceptance</i>	ICTSO, Pentadbir Rangkaian

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	73

<i>Check</i> (FAC) semasa pemasangan dan konfigurasi; e. Firewall hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Rangkaian; f. Semua trafik keluar dan masuk dalam rangkaian PKPP hendaklah melalui firewall di bawah kawalan PKPP; g. Semua perisian <i>sniffer</i> atau <i>network analyser</i> adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h. Memasang perisian <i>Intrusion Prevention System</i> (IPS) atau <i>Web Application Firewall</i> (WAF) mengikut kesesuaian bagi mengesan sebarang cubaan mencerooboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat di dalam rangkaian PKPP; i. Memasang <i>Web Content Filtering</i> untuk menyekat aktiviti <i>Web Surfing</i> yang dilarang semasa waktu kerja; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan PKPP adalah tidak dibenarkan; k. Sebarang penggunaan rangkaian komunikasi daripada agensi lain (contoh: EGNNet, NRENet) perlulah mendapat khidmat nasihat daripada pentadbir rangkaian terlebih dahulu dan pelaksanaan secara berpusat perlulah menjadi keutamaan; l. Kemudahan rangkaian tanpa wayar (<i>wireless</i>) perlu dipantau dan dipastikan kawalan keselamatan serta dikawal penggunaannya; m. Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi <i>Service Level Assurance</i> (SLA) yang telah ditetapkan; n. Menempatkan atau memasang antara muka (<i>interfaces</i>) yang bersesuaian di antara rangkaian PKPP, rangkaian agensi lain dan rangkaian awam; o. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya;	ICTSO, Pentadbir Rangkaian
---	-----------------------------------

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	74

q. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja; r. Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh; s. Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan rangkaian PKPP; dan t. Mewujud dan melaksana kawalan pengalihan laluan (<i>routing control</i>) bagi memastikan pematuhan terhadap peraturan PKPP.	ICTSO, Pentadbir Rangkaian
8.21 KESELAMATAN PERKHIDMATAN RANGKAIAN (SECURITY OF NETWORK SERVICES)	PERANAN
Pengurusan bagi semua perkhidmatan rangkaian (<i>inhouse atau outsource</i>) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian.	ICTSO, Pentadbir Rangkaian, Pembekal
8.22 PENGASINGAN RANGKAIAN (SEGREGATION OF NETWORKS)	PERANAN
Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian PKPP.	ICTSO, Pentadbir Rangkaian
8.23 PENAPISAN LAMAN WEB (WEB FILTERING)	PERANAN
Organisasi harus mewujudkan dan melaksanakan kawalan yang diperlukan untuk menghalang pekerja daripada mengakses laman web luaran yang mungkin mengandungi virus, bahan yang tidak selamat, data atau jenis maklumat haram yang lain dengan: a. Laman web dengan fungsi muat naik maklumat. Akses hendaklah tertakluk kepada kebenaran dan hanya boleh diberikan atas sebab yang sah mengikut Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 atau pekeliling-pekeliling semasa. b. Laman web yang diketahui atau disyaki mengandungi bahan berniat jahat, seperti laman web dengan kandungan perisian yang tidak selamat. c. Pelayan perintah dan kawalan.	ICTSO, Pentadbir Rangkaian, Pentadbir Teknikal

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	75

d. Laman web berniat jahat yang diperoleh daripada <i>scammer</i>. e. Laman web yang mengedarkan kandungan dan bahan yang menyalahi undang-undang.	ICTSO, Pentadbir Rangkaian, Pentadbir Teknikal
8.24 PENGGUNAAN KRIPTOGRAFI (USE OF CRYPTOGRAPHY)	PERANAN
1. Kriptografi merangkumi kaedah-kaedah seperti yang berikut: a. Enkripsi - Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (<i>encryption</i>). b. Tandatangan Digital - Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan. 2. Pengurusan ke atas Pengurusan Infrastruktur Kunci Awam (<i>Public Key Infrastructure</i>) PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	ICTSO, Pentadbir Rangkaian, Pentadbir Teknikal, Warga PKPP
8.25 KITARAN HAYAT PEMBANGUNAN SELAMAT (SECURE DEVELOPMENT LIFE CYCLE)	PERANAN
Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Keselamatan persekitaran pembangunan; b. Keselamatan pangkalan data; c. Keperluan keselamatan dalam fasa reka bentuk; d. Keperluan <i>check point</i> keselamatan dalam carta perbatuan projek; e. Keperluan pengetahuan ke atas keselamatan aplikasi; f. Keselamatan dalam kawalan versi; dan g. Bagi pembangunan secara penyumberluaran (<i>outsource</i>), pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.	ICTSO, Pentadbir Sistem Aplikasi

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	76

8.26 KEPERLUAN KESELAMATAN APLIKASI (APPLICATION SECURITY REQUIREMENTS)	PERANAN
1. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi PKPP. Contoh perkhidmatan sumber luaran ialah: i. Perisian sebagai satu perkhidmatan; ii. platform sebagai satu perkhidmatan; iii. Infrastruktur sebagai satu perkhidmatan; iv. Storan pengkomputeran awan; dan v. Pemantauan keselamatan. b. Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala; c. Tahap kerahsiaan bagi mengenalpasti identiti masing-masing, misalnya melalui pengesahan (<i>authentication</i>); d. proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi; e. Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan f. Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	Pentadbir Sistem Aplikasi, ICTSO, Pengurus ICT
2. Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulang tayang mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi; b. Memastikan semua aspek transaksi dipatuhi: i. maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan; ii. mengekalkan kerahsiaan maklumat; iii. mengekalkan privasi pihak yang terlibat; dan	Pentadbir Sistem Aplikasi

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	77

iv. protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi. c. Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh Kerajaan.	Pentadbir Sistem Aplikasi
8.27 PRINSIP SENIBINA DAN KEJURUTERAAN SISTEM SELAMAT (SECURE SYSTEM ARCHITECTURES AND ENGINEERING PRINCIPLES)	PERANAN
Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpanduan kepada Garis Panduan dan Pelaksanaan <i>Independent Verification and Validation (IV&V)</i> sektor awam yang terkini.	Pentadbir Sistem Aplikasi
8.28 PENGEKODAN SELAMAT (SECURE CODING)	PERANAN
Amalan dan prosedur pengkodan yang selamat hendaklah mengambil kira perkara berikut untuk proses pengkodan: a. Prinsip pengkodan perisian yang selamat harus disesuaikan dengan setiap bahasa pengaturcaraan dan teknik yang digunakan. b. Penggunaan teknik dan kaedah <i>secure coding</i> seperti pembangunan yang hendak dilakukan hendaklah dibuat pengujian dan pemasangan pasangan (<i>pair programming</i>). c. Penggunaan kaedah pengaturcaraan yang berstruktur. d. Dokumentasi kod yang betul dan penyingkiran kecacatan kod. e. Larangan ke atas penggunaan kaedah pengkodan perisian yang tidak selamat seperti sampel kod yang tidak diluluskan atau kata laluan berkod keras (<i>hard coded</i>). f. Kod yang digunakan hendaklah sentiasa dikemaskini mengikut keadaan keselamatan semasa.	Pentadbir Sistem Aplikasi

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	78

8.29 PENGUJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN (<i>SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE</i>)	PERANAN
1. Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; b. Membuat semakan pengesahan di dalam aplikasi untuk mengenalpasti kesilapan maklumat; dan c. Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan. 2. Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; b. Pengujian penerimaan sistem hendaklah merangkumi Keperluan Keselamatan Sistem Maklumat dan kepatuhan kepada Polisi Pembangunan Selamat; c. penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai; dan d. pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan (<i>vulnerability scanner</i>).	ICTSO, Pentadbir Sistem Aplikasi ICTSO, Pentadbir Sistem Aplikasi, Pengguna
8.30 PEMBANGUNAN OLEH PIHAK LUAR (<i>OUTSOURCED DEVELOPMENT</i>)	PERANAN
Pembangunan aplikasi secara <i>outsource</i> perlu diselia dan dipantau oleh pegawai yang dipertanggungjawabkan. Kod sumber (<i>source code</i>) bagi semua aplikasi dan perisian adalah menjadi hak milik PKPP. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Perkiraan perlesenan, kod sumber ialah HAK MILIK PKPP dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara <i>outsource</i>; b. Bagi semua perkhidmatan sumber luaran, perisian sebagai satu	ICTSO, Pentadbir Sistem Aplikasi

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	79

perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori "Pembekal hendaklah membenar Kerajaan hak mencapai 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 kepada kualiti dan ketepatan serahan sistem; e. Menggunakan pakai prinsip dan tatacara <i>escrow</i> (sekiranya perlu); dan f. Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian.	ICTSO, Pentadbir Sistem Aplikasi
8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN , PENGUJIAN DAN OPERASI (SEPARATION OF DEVELOPMENT, TEST AND PRODUCTION ENVIRONMENT)	PERANAN
Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. PKPP perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: a. Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem; b. Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; c. Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem; d. Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; e. Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan f. Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	Pentadbir Sistem Aplikasi

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	80

8.32 PENGURUSAN PERUBAHAN (<i>CHANGE MANAGEMENT</i>)	PERANAN
1. Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perubahan ke atas sistem hendaklah dikawal. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b. aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; c. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d. Keperluan dan kesesuaian perubahan terhadap sistem pengoperasian dan perisian sokongan perlu dikaji terlebih dahulu. e. Sebarang perubahan sistem pengoperasian dan perisian sokongan perlu diuji dahulu di dalam <i>development server</i> sebelum dipasang di dalam server sebenar. f. Akses kepada kod sumber (<i>source code</i>) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan g. Menghalang sebarang peluang untuk membocorkan maklumat.	Pengurus ICT, Pentadbir Sistem Aplikasi
2. Apabila platform operasi berubah, aplikasi penting perniagaan hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan organisasi. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform; b. Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan c. Memastikan perubahan yang sesuai dibuat kepada PKP PKPP dan Pelan Pemulihan Bencana Sistem yang berkaitan berdasarkan Pelan Pengurusan Keselamatan	Pentadbir Sistem Aplikasi

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	81

Maklumat (ISMP) sistem tersebut. 3. Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.	Pengurus ICT,Pentadbir Sistem Aplikasi
8.33 MAKLUMAT UJIAN (TEST INFORMATION)	PERANAN
Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; b. Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian; c. Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan d. Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar.	ICTSO, Pentadbir Sistem Aplikasi
8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PENGUJIAN AUDIT (PROTECTION OF INFORMATION SYSTEMS DURING AUDIT TESTING)	PERANAN
Keperluan dan aktiviti audit yang melibatkan pengujian sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses kelancaran sistem.	ICTSO, Pentadbir Sistem Aplikasi

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	82

GLOSARI

Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, <i>optical disk</i> , <i>flash disk</i> , <i>CDROM</i> , <i>thumb drive</i> untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	LebarJalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam angka masa yang ditetapkan.
CDO	<i>Chief Digital Officer</i> Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
<i>Denial of service</i>	Halangan pemberian perkhidmatan.
<i>Downloading</i>	Aktiviti muat-turun sesuatu perisian.
<i>Encryption</i>	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
<i>Forgery</i>	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (<i>information theft/espionage</i>), penipuan (<i>hoaxes</i>).
CSIRT PKPP	<i>Computer Security Incident Response Team</i> atau Pasukan Tindak Balas Insiden Keselamatan ICT PKPP.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	83

Hub	Hab (hub) 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.
ICT	Information and Communication Technology (Teknologi Maklumat dan Komunikasi)
ICTSO	ICT Security Officer Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
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- rangkaian tersebut agar sentiasa berasingan.
<i>Intrusion Detection System (IDS)</i>	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
<i>Intrusion Prevention System (IPS)</i>	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Contohnya: Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	<i>Local Area Network</i> Rangkaian Kawasan Setempat yang menghubungkan komputer.
<i>Logout</i>	<i>Log-out</i> komputer Keluar daripada sesuatu sistem atau aplikasi komputer
<i>Malicious Code</i>	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, trojan horse, worm, spyware dan sebagainya.

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	84

MODEM	Modulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaianInternet dibuat dari komputer.
<i>Outsource</i>	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi- fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti <i>spreadsheet</i> dan <i>word processing</i> ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
<i>Screen Saver</i>	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakandalam jangka masa tertentu.
Server	Pelayan komputer
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian <i>Carrier Sense Multiple Access/Collision Detection</i> (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaranyang berlaku.
<i>Threat</i>	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif peribadi dan atas sebab tertentu.
<i>Uninterruptible Power Supply</i> (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
<i>Video Conference</i>	Media yang menerima dan memaparkan maklumat multimedia kepadapengguna dalam masa yang sama ia diterima oleh penghantar.
<i>Video Streaming</i>	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.
<i>Wireless LAN</i>	Jaringan komputer yang terhubung tanpa melalui kabel.

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	85

LAMPIRAN 1 : SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER PKPP

Lampiran 1

Polisi Keselamat Siber PKPP
Versi 1.0

**SURAT AKUAN PEMATUHAN POLISI
KESELAMATAN SIBER**

PERBADANAN KEMAJUAN PERTANIAN NEGERI PAHANG

NAMA (HURUF BESAR)	
NO.KAD PENGENALAN	
JAWATAN	
BAHAGIAN/UNIT/ SYARIKAT	

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

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

Tandatangan

Tarikh:

Rujukan : Sila layari Polisi Keselamatan Siber PKPP di <https://www.pkpp.gov.my>

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	86

**LAMPIRAN 2 : SURAT PERAKUAN PEMATUHAN AKTA RAHSIA RASMI 1972 [AKTA 88]
DAN POLISI KESELAMATAN SIBER PKPP**



**SURAT PERAKUAN PEMATUHAN AKTA RAHSIA RASMI 1972 [AKTA 88] DAN POLISI
KESELAMATAN SIBER PKPP**

**PERAKUAN UNTUK DITANDATANGANI BERKENAAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88] DAN
POLISI KESELAMATAN SIBER PKPP**

NAMA PROJEK :

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu rahsia atau apa-apa tingkah laku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi sesuatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

Saya faham bahawa segala maklumat rasmi yang saya perolehi adalah milik PKPP dan tidak akan membocorkan, menyiarkan atau menyampaikan, sama ada secara lisan atau dengan bertulisan atau secara media elektronik, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapatkan kebenaran bertulis pihak berkuasa yang berkenaan.

Saya juga turut tertakluk di bawah Polisi Keselamatan Siber PKPP terkini berkenaan Perkara: Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal. Selain itu, saya juga telah membaca dan faham serta akan mematuhi polisi lain di dalam Polisi Keselamatan Siber PKPP yang berhubungkait dengan urusan ini.

Saya juga dengan ini mewakili

mengakui bahawa semua maklumat yang dinyatakan seperti di Lampiran A adalah terlibat secara langsung bagi sebarang urusan yang memerlukan pematuhan akta dan Polisi Keselamatan Siber PKPP

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	87

seperti semua keterangan perenggan di atas. Oleh itu, sesiapa yang tiada dalam senarai Lampiran A tersebut tidak dibenarkan terlibat secara langsung bagi sebarang urusan melibatkan peruntukan Akta Rahsia Rasmi 1972 [Akta 88].

Sila lengkapkan dengan tulisan HURUF BESAR			
Tandatangan		Disaksikan Oleh	
Nama		Nama	
No.Kad Pengenalan		No.Kad Pengenalan	
Jawatan		Jawatan	
Jabatan/Syarikat		Jabatan/Syarikat	
Tarikh		Tarikh	
Alamat		Cop Jabatan/Syarikat	

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	88

LAMPIRAN A



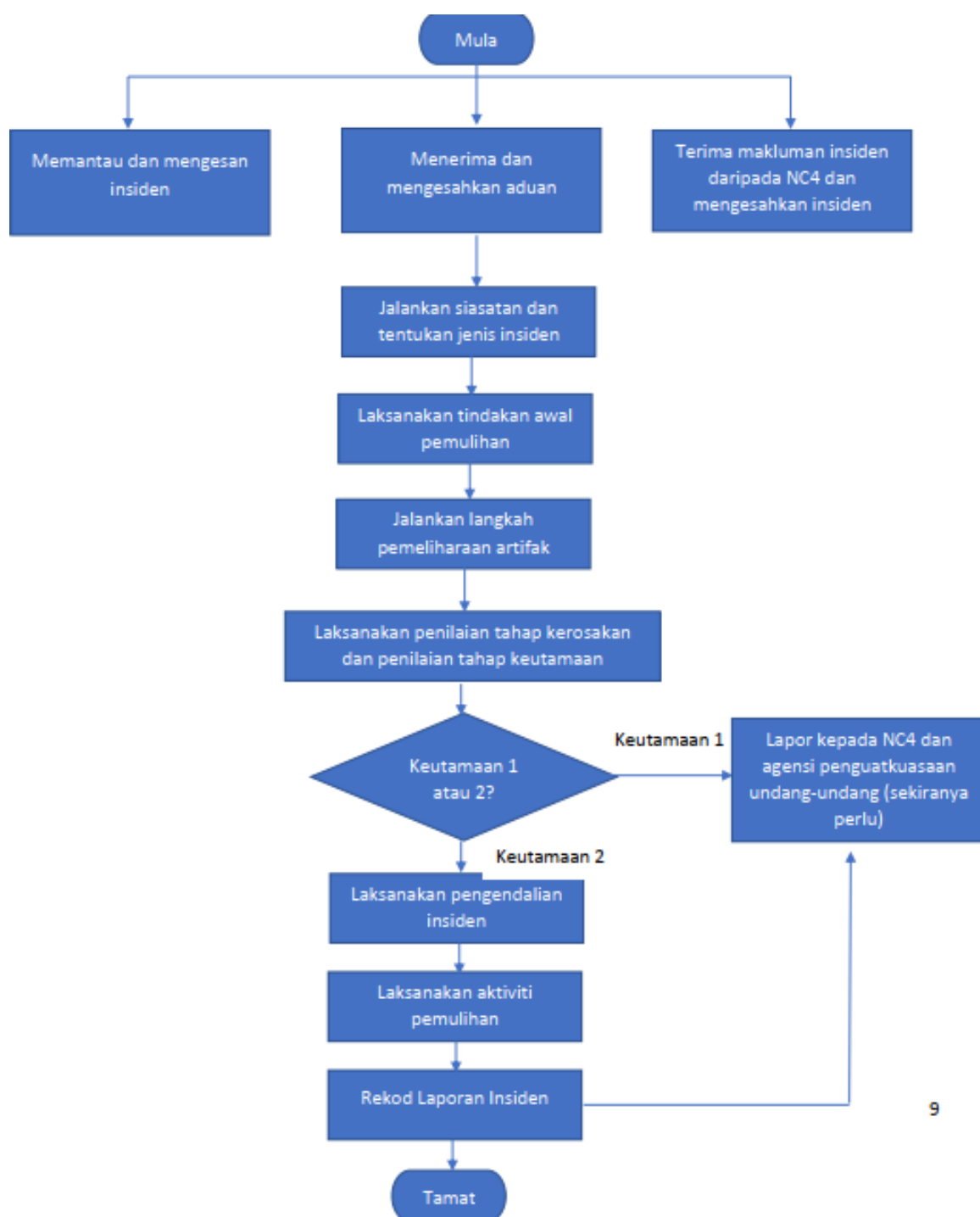
SENARAI KAKITANGAN JABATAN / SYARIKAT YANG TERLIBAT DALAM URUSAN ANTARA JABATAN / SYARIKAT DENGAN PKPP TERLIBAT

* Sila lengkapkan dengan tulisan HURUF BESAR

Bil	Nama & Jabatan	Jawatan Syarikat	No. K/P

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	89

LAMPIRAN 3 : PROSES KERJA PELAPORAN INSIDEN KESELAMATAN SIBER PKPP



9

RUJUKAN	REVISI	TARIKH	M/SURAT
PKS PKPP	Versi 1.0	13/11/2025	90

LAMPIRAN 4 : SENARAI PERUNDANGAN DAN PERATURAN

1. Arahan Keselamatan (Semakan dan Pindaan 2017);
2. Akta Rahsia Rasmi 1972 [Akta 88];
3. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
4. Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam bertarikh 24 Nov 2010
5. Surat Arahan Ketua Pengarah MAMPU - Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC27001:2007 dalam Sektor Awam bertarikh 24 Nov 2010
6. Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (GCERT) oleh NACSA bertarikh 28 Januari 2019
7. Surat Pemakluman Pengurusan Maklumat Pegawai Keselamatan ICT (ICTSO) Sektor Awam bertarikh 28 Februari 2019
8. Surat Pemakluman Kaedah Pelaksanaan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 6 April 2022
9. Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022
10. Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024
11. Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024
12. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) V1.0 MAMPU (April 2016)
13. Akta Tandatangan Digital 1997 [Akta 562];
14. Akta Jenayah Komputer 1997 [Akta 563];
15. Perintah-perintah Am;
16. Akta Hak Cipta (Pindaan) 2022;
17. Akta Komunikasi dan Multimedia 1998 [Akta 588];
18. Arahan Perbendaharaan (Pindaan 2023);
19. 1PP/AM1.1 Pekeliling Perbendaharaan Malaysia – Pengurusan Aset Kerajaan
20. 1PP/PK2 Pekeliling Perbendaharaan Malaysia – Kaedah Perolehan Kerajaan
21. Akta Keselamatan Siber 2024 dan Peraturan-peraturan [Akta 854]