KEMENTERIAN
KEMAJUAN DESA DAN WILAYAH

POLISI KESELAMATAN SIBER

VERSI 6.0





KEMENTERIAN KEMAJUAN DESA DAN WILAYAH

POLISI KESELAMATAN SIBER KEMENTERIAN KEMAJUAN DESA DAN WILAYAH		
DOKUMEN DISEDIAKAN OLEH	**:**	UNIT KESELAMATAN DAN PEMULIHAN BENCANA, BAHAGIAN PENGURUSAN MAKLUMAT
VERSI DOKUMEN	**:**	6.0
TARIKH DOKUMEN	**:**	27 NOVEMBER 2025
KLASIFIKASI DOKUMEN	**:**	TERBUKA
Hak cipta terpelihara Kerajaan Malaysia		

Dokumen ini telah disemak dan diterima oleh pihak yang berikut:

PENGESAHAN DOKUMEN		
Disediakan Oleh	:	**Tandatangan: .....** Nama: **Yusliana binti Adnan** Jawatan/Peranan: Penolong Setiausaha Tarikh: 20 Oktober 2025
Disemak Oleh	:	**Tandatangan: .....** Nama: **Mohd Surizalman bin Mohd Zain** Jawatan/Peranan: Ketua Penolong Setiausaha Tarikh: 27 Oktober 2025
Disahkan Oleh	:	**Tandatangan: .....** Nama: **Azizah binti Abd Kadir** Jawatan/Peranan: SUB(ICT) Tarikh: 31 Oktober 2025
Diluluskan Oleh	:	**Tandatangan: .....** Nama: **Dato' Dr Roslan bin Mahmood** Jawatan/Peranan: CDO Tarikh: 14 November 2025

PRAKATA

Bismillahirrahmanirrahim,

Assalamualaikum warahmatullahi wabarakatuh dan Salam Sejahtera,

Alhamdulillah, dengan izin dan limpah kurnia-Nya, Kementerian Kemajuan Desa dan Wilayah (KKDW) berjaya menerbitkan **Polisi Keselamatan Siber Versi Baharu** ini sebagai satu rujukan rasmi dalam memperkukuh tahap keselamatan maklumat di kementerian kita.

Dunia digital masa kini berkembang pantas dan membawa bersama pelbagai cabaran keselamatan siber yang semakin kompleks. Ancaman terhadap sistem, data, dan maklumat rasmi kementerian tidak lagi bersifat konvensional, malah memerlukan pendekatan keselamatan yang lebih holistik, dinamik, dan bersepadu. Justeru, penerbitan versi baharu ini merupakan langkah proaktif KKDW untuk memastikan bahawa setiap aset maklumat kekal terpelihara, dipercayai dan dilindungi daripada sebarang bentuk ancaman atau penyalahgunaan.

Dokumen ini dirangka berasaskan garis panduan dan amalan terbaik keselamatan siber semasa, termasuklah pematuhan kepada Dasar Keselamatan Siber Nasional (DKSN) serta standard antarabangsa yang relevan. Ia menjadi panduan utama kepada semua pegawai dan warga kerja KKDW dalam memahami peranan, tanggungjawab, serta prosedur dalam mengurus keselamatan maklumat seharian.

Saya menyeru semua warga kementerian agar menjadikan polisi ini sebagai sebahagian daripada budaya kerja seharian. Kepatuhan dan pelaksanaan polisi ini bukan sahaja tanggungjawab individu, malah ia mencerminkan komitmen kita secara kolektif untuk memastikan KKDW sentiasa kukuh dan berwibawa dalam era digital ini.

Akhir kata, saya merakamkan setinggi-tinggi penghargaan kepada semua pihak yang terlibat dalam penyediaan dokumen penting ini. Semoga usaha kita diberkati dan menjadi asas kukuh kepada pengurusan keselamatan maklumat yang lebih cemerlang di KKDW.

Sekian, terima kasih.

Dato' Dr. Roslan bin Mahmood
Ketua Pegawai Digital (CDO)
Kementerian Kemajuan Desa dan Wilayah (KKDW)

ISI KANDUNGAN

PRAKATA 4
ISI KANDUNGAN 5
MAKLUMAT DAN KAWALAN DOKUMEN 11
1 PENDAHULUAN 13
1.1 PENGENALAN 13
1.2 TUJUAN 13
1.3 OBJEKTIF 14
1.4 SKOP 14
2 TADBIR URUS 19
3 PENGURUSAN RISIKO KESELAMATAN MAKLUMAT 23
4 POLISI DAN OBJEKTIF KESELAMATAN 26
4.1 PERNYATAAN POLISI 26
4.2 PRINSIP KESELAMATAN 27
5 KAWALAN ORGANISASI (*ORGANIZATIONAL CONTROL*) 32
5.1 Polisi Keselamatan Siber 32
(*Cyber Security Policy*) 32
5.2 Peranan dan Tanggungjawab Keselamatan Maklumat 34
(*Information Security Roles and Responsibilities*) 34
5.3 Pengasingan Tugas 42
(*Segregation of Duties*) 42
5.4 Tanggungjawab Pengurusan 43
(*Management Responsibilities*) 43
5.5 Hubungan dengan Pihak Berkuasa 44
(*Contact with Authorities*) 44
5.6 Hubungan Dengan Kumpulan Berkepentingan Yang Khusus 45
(*Contact with Special Interest Groups*) 45
5.7 Perisikan Ancaman 46
(*Threat Intelligence*) 46
5.8 Keselamatan Maklumat dalam Pengurusan Projek 47
(*Information Security in Project Management*) 47
5.9 Inventori Maklumat dan Aset Lain yang Berkaitan 49
(*Inventory of Information and Other Associated Assets*) 49
5.10 Penggunaan Maklumat yang Boleh Diterima dan Aset Lain yang Berkaitan
(*Acceptable Use of Information and Other Associated Assets)* 51
5.11 Pemulangan Aset 52

(*Return of Assets*) 52
5.12 Pengelasan Maklumat 52
(*Classification of Information*) 52
5.13 Pelabelan Maklumat 54
(*Labelling of Information*) 54
5.14 Pemindahan Data dan Maklumat 55
(*Information Transfer*) 55
5.15 Kawalan Capaian 57
(*Access control*) 57
5.16 Pengurusan Identiti 61
(*Identity Management*) 61
5.17 Maklumat Pengesahan 63
(*Authentication Information*) 63
5.18 Hak Capaian 67
(*Access Rights*) 67
5.19 Keselamatan Maklumat Dalam Hubungan Pembekal 70
(*Information Security in Supplier Relationships*) 70
5.20 Menangani Keselamatan dalam Perjanjian dengan Pembekal 72
(*Addressing Security within Supplier Agreements*) 72
5.21 Menguruskan Keselamatan Maklumat dalam Rantaian Bekalan Teknologi Maklumat dan Komunikasi 74
(*Managing Information Security in The Information and Communication Technology (ICT) Supply Chain*) 74
5.22 Memantau, Menyemak dan Mengubah Pengurusan Perkhidmatan Pembekal 75
(*Monitoring, Review and Change Management of Supplier Services*) 75
5.23 Keselamatan Maklumat bagi Penggunaan Perkhidmatan Awan (*Information Security for Use of Cloud Services*) 76
5.24 Perancangan dan Penyediaan Pengurusan Insiden Keselamatan Maklumat (*Information Security Incident Management Planning and Preparation*) 77
5.25 Penilaian dan Keputusan mengenai Kejadian Keselamatan Maklumat (*Assessment of and Decision on Information Security Events*) 78
5.26 Tindak Balas Terhadap Insiden Keselamatan Maklumat 79
(*Response to Information Security Incidents*) 79
5.27 Pembelajaran Daripada Insiden Keselamatan Maklumat 80
(*Learning from Information Security Incidents*) 80
5.28 Pengumpulan Bahan Bukti 81
(*Collection of Evidence*) 81
5.29 Keselamatan Maklumat Semasa Gangguan 81

(*Information Security During Disruption*) 81
5.30 Kesediaan ICT Bagi Kesinambungan Perkhidmatan 83
(*ICT Readiness for Business Continuity*) 83
5.31 Keperluan Perundangan dan Kontrak 87
(*Legal, Statutory, Regulatory and Contractual Requirements*) 87
5.32 Hak Harta Intelek 88
(*Intellectual Property Rights*) 88
5.33 Perlindungan Rekod 88
(*Protection of Records*) 88
5.34 Privasi dan Perlindungan Peribadi yang boleh dikenal pasti 89
(*Privacy and Protection of Personal Identifiable Information* (PII)) 89
5.35 Kajian Semula Keselamatan Maklumat Secara Berkecuali 89
(*Independent Review of Information Security*) 89
5.36 Pematuhan Dasar, Peraturan dan Piawaian Untuk Keselamatan Maklumat (*Compliance With Policies, Rules and Standards for Information Security*) 90
5.37 Dokumentasi Prosedur Operasi yang Didokumenkan 91
(*Documented Operating Procedures*) 91
6 KAWALAN SUMBER MANUSIA (*PEOPLE CONTROL*) 94
6.1 Tapisan Keselamatan 94
(*Security Screening*) 94
6.2 Terma dan Syarat Perkhidmatan 95
(*Terms and Conditions of Employment*) 95
6.3 Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat (*Information Security Awareness, Education and Training*) 95
6.4 Proses Tatatertib 96
(*Disciplinary Process*) 96
6.5 Tanggungjawab selepas Penamatan atau Pertukaran Pekerjaan (*Responsibilities after Termination or Change of Employment*) 97
6.6 Perjanjian Kerahsiaan atau Ketakdedahan 98
(*Confidentiality Or Non-Disclosure Agreements*) 98
6.7 Bekerja Jarak Jauh 99
(*Remote Working*) 99
6.8 Pelaporan Insiden Keselamatan Maklumat 99
(*Reporting Information Security Events*) 99
7 KAWALAN FIZIKAL (*PHYSICAL CONTROL*) 102
7.1 Perimeter Keselamatan Fizikal 102
(*Physical Security Parameter*) 102

7.2 Kemasukan Fizikal 103
(*Physical Entry*) 103
7.3 Keselamatan Pejabat, Bilik dan Kemudahan 105
(*Securing Offices, Rooms and Facilities*) 105
7.4 Pemantauan Keselamatan Fizikal 105
(*Physical Security Monitoring*) 105
7.5 Perlindungan Daripada Ancaman Fizikal Dan Persekitaran 106
(Protecting Against Physical and Environmental Threats) 106
7.6 Bekerja di Kawasan Selamat 107
(*Working In Secure Areas*) 107
7.7 Meja Kosong dan Skrin Kosong 108
(*Clear Desk and Clear Screen*) 108
7.8 Penempatan dan Perlindungan Peralatan ICT 110
(*Equipment Siting and Protection*) 110
7.9 Keselamatan Aset di Luar Premis 112
(*Security of Assets Off-Premises*) 112
7.10 Media Storan 113
(*Storage Media*) 113
7.11 Utiliti Sokongan 115
(*Supporting Utilities*) 115
7.12 Keselamatan Kabel 115
(*Cabling Security*) 115
7.13 Penyelenggaraan Peralatan 116
(*Equipment Maintenance*) 116
7.14 Pelupusan yang Selamat atau Penggunaan Semula Peralatan 117
(*Secure Disposal or Re-Use of Equipment*) 117
8 KAWALAN TEKNOLOGI (*TECHNOLOGICAL CONTROL*) 121
8.1 Peranti Titik Hujung Pengguna 121
(*User Endpoint Devices*) 121
8.2 Hak Akses Istimewa 122
(*Privileged Access Rights*) 122
8.3 Sekatan Akses Maklumat 122
(*Information Access Restriction*) 122
8.4 Kawalan Akses kepada Kod Sumber Program 124
(*Access Control to Source Code*) 124
8.5 Pengesahan Selamat 124
(*Secure Authentication*) 124

8.6 Pengurusan Kapasiti 127
(*Capacity Management*) 127
8.7 Perlindungan daripada Perisian Hasad 127
(*Protection Against Malware*) 127
8.8 Pengurusan Kerentanan Teknikal 129
(*Management of Technical Vulnerabilities*) 129
8.9 Pengurusan konfigurasi 130
(*Configuration Management*) 130
8.10 Penghapusan Maklumat 131
(*Information Deletion*) 131
8.11 Penyamaran Data 131
(*Data Masking*) 131
8.12 Pencegahan Ketirisan Data 132
(*Data Leakage Prevention*) 132
8.13 Sandaran Maklumat 133
(*Information Backup*) 133
8.14 Lewahan bagi Kemudahan Pemprosesan Maklumat 134
(*Redundancy of Information Processing Facilities*) 134
8.15 Menyediakan Log 134
(*Logging*) 134
8.16 Aktiviti Pemantauan 137
(*Monitoring Activities*) 137
8.17 Penyeragaman Jam 138
(*Clock Synchronization*) 138
8.18 Penggunaan Program Utiliti yang Mempunyai Hak Istimewa 138
(*Use of Privileged Utility Programs*) 138
8.19 Pemasangan Perisian pada Sistem yang Beroperasi 139
(*Installation of Software on Operational Systems*) 139
8.20 Keselamatan Rangkaian 141
(*Networks Security*) 141
8.21 Keselamatan Perkhidmatan Rangkaian 142
(*Security of Network Services*) 142
8.22 Pengasingan dalam Rangkaian 143
(*Segregation of Networks*) 143
8.23 Penyaringan Web 143
(*Web Filtering*) 143
8.24 Penggunaan Kriptografi 144

(*Use of Cryptography*) 144
8.25 Kitar Hayat Pembangunan Sistem yang Selamat 145
(*Secure Development Life Cycle*) 145
8.26 Keperluan Keselamatan Aplikasi 147
(*Application Security Requirements)* 147
8.27 Prinsip Reka Bentuk dan Kejuruteraan Sistem yang Selamat 148
(*Secure System Architecture and Engineering Principles*) 148
8.28 Pengekodan Selamat 149
(*Secure Coding*) 149
8.29 Pengujian dan Penerimaan Keselamatan Sistem 150
(*Security Testing in Development and Acceptance*) 150
8.30 Pembangunan oleh Pembekal 151
(*Outsourced Development*) 151
8.31 Pengasingan Persekitaran Pembangunan, Pengujian dan Pengeluaran (*Separation of Development, Test and Production Environments*) 153
8.32 Pengurusan Perubahan 155
(*Change Management*) 155
8.33 Data Pengujian 157
(*Test Information*) 157
8.34 Perlindungan Sistem Maklumat Semasa Pengujian Audit 158
(*Protection of Information Systems During Audit Testing*) 158
LAMPIRAN A 161
LAMPIRAN B 162
LAMPIRAN C 163

MAKLUMAT DAN KAWALAN DOKUMEN

Polisi Keselamatan Siber (PKS) ialah satu set garis panduan dan prosedur yang direka bentuk untuk melindungi aset digital, maklumat dan infrastruktur teknologi Kementerian Kemajuan Desa dan Wilayah (KKDW) daripada ancaman siber. Ia menggariskan peraturan dan prosedur yang perlu dipatuhi oleh semua pihak berkepentingan untuk melindungi rangkaian, sistem dan data KKDW daripada akses tanpa kebenaran, pelanggaran, dan serangan siber. PKS yang ditakrifkan merangkumi peruntukan untuk penilaian risiko, pengurusan kelemahan, perlindungan data, tindak balas insiden, keistimewaan pengguna dan pematuhan undang-undang dan peraturan yang berkaitan. Ia berfungsi sebagai rangka kerja penting untuk menerapkan amalan terbaik keselamatan maklumat dan memastikan kerahsiaan, integriti dan ketersediaan sumber kritikal dalam KKDW.

REKOD PINDAAN DOKUMEN

Tarikh	Versi	Kelulusan	Tarikh Kuat Kuasa
17 SEPT 2007	1.0	JPICT BIL.3/2007	18 SEPT 2007
23 MAC 2010	2.0	JPICT BIL.2/2010	24 MAC 2010
23 MEI 2014	3.0	JPICT BIL.3/2014	24 MEI 2014
21 MEI 2018	4.0	JPICT BIL.3/2018	21 MEI 2018
25 JAN 2022	5.0	JPICT BIL.1/2022	25 JAN 2022
20 NOV 2023	5.1	JPICT BIL.4/2023	20 NOV 2023
21 NOV 2025	6.0	JPICT BIL.4/2025	27 NOV 2025

#1 PENDAHULUAN



1 PENDAHULUAN

1.1 PENGENALAN

Polisi Keselamatan Siber (PKS) Kementerian Kemajuan Desa dan Wilayah (KKDW) adalah dokumen yang menunjukkan hala tuju jelas KKDW dalam memastikan keselamatan maklumat secara komprehensif. Polisi ini telah pun mendapat kelulusan rasmi daripada pengurusan KKDW untuk dilaksanakan di Kementerian ini.

Dokumen ini disediakan untuk menjaga kerahsiaan, integriti, dan ketersediaan maklumat di Kementerian**.** Ia mengandungi kumpulan arahan, peraturan-peraturan, garis panduan, dan amalan yang ditetapkan untuk melindungi maklumat dan data yang sensitif serta penting daripada capaian yang tidak sah, kehilangan atau pengungkapan yang tidak dibenarkan.

PKS KKDW yang dinyatakan dalam dokumen ini, mentakrif kawalan yang bersesuaian berdasarkan dasar/pekeliling/garis panduan kerajaan semasa yang berkuat kuasa dan amalan terbaik keselamatan yang terpakai pada sistem dan persekitaran maklumat dalam ruangan siber.

1.2 TUJUAN

PKS KKDW dibangunkan untuk mewujudkan rangka kerja yang komprehensif dalam melindungi aset maklumat KKDW daripada ancaman dan kerentanan yang mungkin timbul. PKS KKDW bertujuan menerangkan peranan, tanggungjawab, arahan, peraturan-peraturan, garis panduan, dan amalan yang **MESTI DIBACA, DIFAHAMI dan DIPATUHI** oleh warga Kementerian**,** pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT KKDW dalam melindungi maklumat di ruang siber.

Dengan wujudnya PKS KKDW ini, diharapkan pengurusan keselamatan data dan maklumat di Kementerian ini akan menjadi lebih efisien dan efektif, serta dapat meningkatkan tahap jaminan keselamatan yang lebih tinggi.

1.3 OBJEKTIF

Objektif utama PKS KKDW ini adalah seperti berikut:

a) Memastikan keselamatan penyampaian perkhidmatan KKDW berada di tahap tertinggi dan meningkatkan tahap keyakinan pihak berkepentingan yang ingin berurusan dengan Kementerian;
b) Mematuhi keperluan perundangan, peraturan, standard, pekeliling dan prosedur yang sedang berkuat kuasa;
c) Melaksanakan pengurusan risiko dan insiden keselamatan siber yang lebih berkesan;
d) Memastikan kelancaran operasi serta menjamin kesinambungan perkhidmatan Kementerian dengan meminimumkan kesan insiden keselamatan maklumat secara fizikal dan logikal;
e) Memudahkan perkongsian maklumat yang selamat dan terjamin;
f) Mencegah sebarang penyalahgunaan atau kecurian maklumat kerajaan;
g) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan yang berlaku daripada segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan
h) Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

1.4 SKOP

PKS KKDW ini adalah terpakai bagi semua **Aset Maklumat** KKDW yang terdiri daripada data dan maklumat sama ada dalam bentuk salinan digital (*softcopy*) atau salinan bercetak (*hardcopy*), perkakasan (*hardware*), perisian (*software*), infrastruktur ICT, manusia dan premis. Aset-aset ini amat berharga dan penting untuk membolehkan KKDW menjalankan urusan rasmi Kerajaan dengan lancar kepada pemegang taruh dan pihak berkepentingan. Dengan itu, PKS KKDW menetapkan keperluan-keperluan asas seperti berikut:

a) **Kebolehcapaian Data dan Maklumat:** Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan dengan cara yang boleh dipercayai. Ini adalah penting bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan

b) **Kerahsiaan dan Kesempurnaan Maklumat:** Semua data dan maklumat hendaklah dilindungi kerahsiaannya dan dikendalikan dengan baik pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan Aset Maklumat terjamin keselamatannya sepanjang masa, PKS KKDW ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujudkan, dijana, diproses, disimpan, dikongsi, dicetak, diakses, diedarkan, dalam proses penghantaran, diselenggarakan, dimusnahkan, dihapuskan dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur pengendalian semua perkara berikut:

a) **Data atau Maklumat**

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

b) **Salinan Digital (*Softcopy*)**

Koleksi salinan fakta-fakta dalam bentuk digital atau elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif Kementerian. Contohnya, rekod-rekod digital, profil pelanggan, pangkalan data dan fail-fail data, maklumat arkib dan lain-lain.

c) Salinan Bercetak (*Hardcopy*)

Koleksi salinan fizikal fakta-fakta dalam bentuk kertas atau bercetak, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif Kementerian**.** Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod, profil pelanggan, fail-fail dan lain-lain.

d) Perkakasan (*Hardware*)

Semua aset fizikal yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan Kementerian. Contohnya, komputer, pelayan, peralatan komunikasi dan sebagainya.

e) Perisian (*Software*)

Arahan program dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan dalam sistem ICT. Contohnya, perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat Kementerian.

f) Infrastruktur ICT

Merujuk kepada set lengkap perkakasan, perisian, rangkaian, dan kemudahan yang membolehkan penghantaran, penyimpanan, pemprosesan dan mendapatkan semula maklumat dalam organisasi atau merentasi pelbagai organisasi. Ia termasuk sistem komputer, pelayan, pangkalan data, rangkaian (kedua-dua kawasan tempatan dan luas), sambungan Internet, sistem komunikasi, pusat data, perkhidmatan pengkomputeran awan (*cloud computing*) serta peralatan dan teknologi lain yang diperlukan. Infrastruktur ICT yang direka bentuk dan disediakan untuk menyokong dan membolehkan pelbagai jenis perkhidmatan dan aplikasi teknologi maklumat dan komunikasi dalam KKDW yang berfungsi bagi mencapai objektif dan misi Kementerian. Infrastruktur ICT ini termasuk:

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;

ii. Sistem halangan akses seperti sistem kad akses;
iii. Perkhidmatan pengkomputeran awam (SaaS/PaaS/IaaS): dan
iv. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

g) Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian bahagian bagi mencapai misi dan objektif Kementerian. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan peranan yang dilaksanakan; dan

h) Premis

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a) - (g) di atas mesti dilindungi dengan sewajarnya.

Setiap perkara di atas perlu diberi perlindungan rapi untuk mencegah kebocoran rahsia atau kelemahan perlindungan, yang akan dianggap sebagai perlanggaran keselamatan.

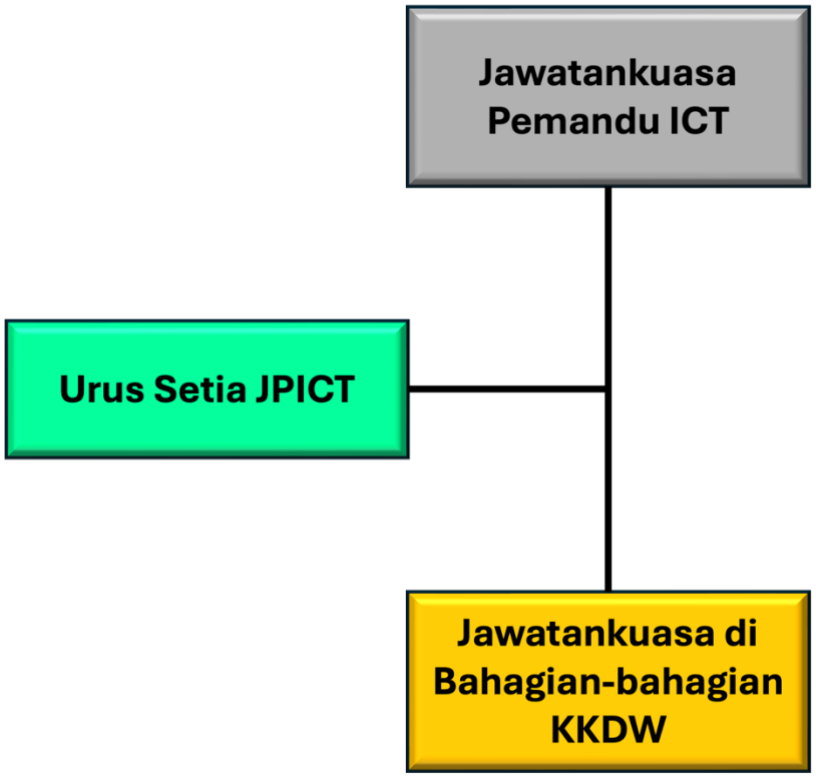
#2 TADBIR URUS



PKS KKDW V6

2 TADBIR URUS

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



Rajah 1: Struktur Jawatankuasa Pemandu ICT KKDW

a) Keahlian Jawatankuasa ini adalah seperti yang berikut:

Pengerusi: Ketua Setiausaha (KSU)

Ahli:

i. Timbalan Ketua Setiausaha (TKSU);
ii. Ketua Pegawai Digital (CDO);
iii. Setiausaha Bahagian (SUB);
iv. Ketua Unit;
v. Ketua Agensi;

vi. Pengurus ICT Agensi; dan

vii. Pegawai Keselamatan ICT (ICTSO) Kementerian.

Urus setia:

Bahagian Pengurusan Maklumat

b) Bidang rujukan JPICT adalah seperti yang berikut:

i. Menetapkan hala tuju dan strategi untuk pembangunan dan pelaksanaan projek ICT KKDW dan semua Agensi di bawahnya;

ii. Mengesahkan cadangan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan projek ICT KKDW dan semua Agensi di bawahnya;

iii. Merancang, menyelaras dan menyeragamkan pembangunan dan pelaksanaan projek ICT KKDW dan semua Agensi di bawahnya supaya selaras dengan pelan strategik organisasi, Pelan Strategik Pendigitalan Kementerian/Agensi, Pelan Strategik Pendigitalan Sektor Awam (PSPSA) atau pelan yang setara;

iv. Menilai dan melulus semua cadangan perolehan ICT KKDW dan Agensi di bawahnya berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan-peraturan semasa yang berkaitan;

v. Menyelaras dan mengemukakan kertas cadangan perolehan ICT bagi KKDW dan semua Agensi di bawahnya kepada JTISA untuk kelulusan teknikal berdasarkan had nilai yang ditetapkan;

vi. Memastikan pelaksanaan projek ICT dipantau dan dilaporkan melalui sistem yang disediakan oleh Jabatan Digital Negara;

vii. Mempromosi dan menggalakkan perkongsian pintar sistem ICT antara KKDW dan semua Agensi di bawahnya;

viii. Merancang, menyelaras, menilai dan meluluskan dasar dan inisiatif keselamatan ICT KKDW dan Agensi di bawahnya;

ix. Memastikan keselarasan projek ICT agar tiada duplikasi dan pembaziran sumber; dan

x. Mengadakan mesyuarat secara berkala (minimum 4 kali setahun) selaras dengan Surat Pekeliling Am Bilangan 7 Tahun 2024 iaitu Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT).

#3

PENGURUSAN RISIKO KESELAMATAN MAKLUMAT



PKS KKDW V6

3 PENGURUSAN RISIKO KESELAMATAN MAKLUMAT

Semua pihak yang terlibat dalam pengurusan data dan maklumat di KKDW hendaklah mengambil kira kewujudan risiko ke atas aset maklumat akibat daripada kelemahan (*vulnerability*) dan ancaman yang semakin meningkat masa kini. Langkah-langkah proaktif dan bersesuaian perlulah diambil tindakan untuk menilai tahap risiko aset maklumat supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan yang optimum.

Penilaian risiko keselamatan maklumat dilaksanakan secara berkala sekurang-kurangnya sekali setahun. Tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan maklumat akan diambil berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan maklumat haruslah dilaksanakan ke atas maklumat KKDW termasuk aset fizikal, aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur yang berkaitan. Penilaian risiko juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuk pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

Pengurusan risiko keselamatan maklumat adalah selaras dengan keperluan yang dinyatakan dalam Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024. Langkah-langkah sewajarnya bagi menghadapi kemungkinan risiko boleh dilakukan dengan memilih tindakan berikut:

a) Mengurangkan (*Reduce*) risiko dengan melaksanakan kawalan yang bersesuaian;
b) Menerima (*Accept*) dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan kementerian;
c) Mengelak (*Avoid*) dan / atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan

d) Memindahkan (*Transfer*) risiko kepada pihak lain seperti pembekal dan pihak lain yang berkepentingan.

Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya **sekali setahun** dalam mesyuarat yang bersesuaian.

#4

POLISI DAN OBJEKTIF KESELAMATAN



PKS KKDW V6

4 POLISI DAN OBJEKTIF KESELAMATAN

4.1 PERNYATAAN POLISI

Aset maklumat adalah aset kritikal yang bernilai kepada KKDW dan oleh itu harus dilindungi dengan sewajarnya. Keselamatan Aset maklumat ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan Aset Maklumat adalah suatu proses yang berterusan dan melibatkan aktiviti berkala yang mesti dilakukan dari masa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan siber sentiasa berubah.

Perlindungan aset maklumat ini merangkumi perlindungan semua bentuk maklumat dan data elektronik yang diwujudkan, dimusnahkan, disimpan, dijana, dicetak, diakses, diedarkan dalam penghantaran dan yang dibuat salinan. Hal ini, bagi memelihara keselamatan aset maklumat dalam ruang siber untuk memastikan kerahsiaan, integriti, tidak boleh disangkal, kesahihan dan ketersediaan capaian aset maklumat kepada semua pengguna yang dibenarkan. Penjelasan ciri-ciri utama keselamatan aset maklumat yang perlu dijaga 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.

Penetapan kawalan keselamatan yang sesuai hendaklah berdasarkan klasifikasi data dan maklumat atau nilai / kepentingan aset maklumat. Klasifikasi data dan maklumat ini boleh merujuk kepada pekeliling / arahan / garis panduan kerajaan yang dikuatkuasakan. Kawalan keselamatan dan langkah-langkah pencegahan hendaklah diambil untuk meminimumkan risiko ancaman yang wujud.

Keselamatan aset maklumat adalah tanggungjawab semua warga Kementerian dan semua pihak yang mempunyai urusan dengan perkhidmatan ICT KKDW.

4.2 PRINSIP KESELAMATAN

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

a) Akses Atas Dasar Perlu Mengetahui

Akses terhadap penggunaan aset maklumat hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15.

b) Hak Akses Minimum

Pengguna hendaklah diberikan hak akses minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak akses atau capaian sistem hendaklah dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu adalah berdasarkan peranan tersebut. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan, tanggungjawab dan bidang tugas pengguna.

c) Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset maklumat KKDW. Tanggungjawab ini perlu dinyatakan dengan jelas dan sesuai dengan tahap sensitiviti sesuatu sumber / aset maklumat. Untuk menentukan tanggungjawab ini dipatuhi, prosedur kerja yang jelas

berupaya untuk mengesan dan mengesahkan tindakan mereka. Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan kata laluan;
v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

d) Pengasingan Tugas

Bagi mengekalkan prinsip semak dan imbang (*check and balance*), KKDW hendaklah melaksanakan pengasingan tugas khususnya bagi tugasan kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data perlu diasingkan mengikut keperluan bagi mengelak daripada capaian yang tidak dibenarkan. Ini bagi melindungi aset maklumat daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian, keselamatan dan aplikasi mengikut kesesuaian.

e) Prinsip Kepercayaan Sifar (*zero trust*)

Prinsip ini menegaskan bahawa tiada pengguna, peranti, atau rangkaian harus dipercayai secara automatik, sama ada berada dalam atau luar perimeter

rangkaian. Setiap permintaan untuk mencapai data atau maklumat mesti melalui proses pengesahan yang teliti sebelum hak capaian diberikan. Prinsip ini menekankan perkara-perkara berikut:

i. semua trafik rangkaian (dalaman dan luaran) dianggap sebagai tidak dipercayai;
ii. akses kepada sumber diberikan berdasarkan set kriteria yang komprehensif, termasuk identiti pengguna, kesihatan peranti, lokasi capaian dan faktor-faktor lain yang bersesuaian. Akses kepada sumber hanya diberikan setelah pengesahan pengguna yang didaftarkan berjaya; dan
iii. menekankan prinsip keistimewaan yang terhad kepada sumber yang perlu diakses, tujuan, apabila diperlukan dan dalam tempoh masa yang diperlukan sahaja.

f) Pengauditan

Pengauditan ialah tindakan untuk menilai, memeriksa, serta menganalisis aktiviti, rekod dan proses yang telah dilaksanakan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Tujuannya adalah untuk memastikan bahawa aktiviti tersebut mematuhi peraturan, piawaian, dan prosedur yang ditetapkan serta untuk mengidentifikasi sebarang isu, ketidakpatuhan, atau potensi risiko. Oleh itu, aset maklumat seperti komputer, pelayan, penghala rangkaian (*network router*), tembok keselamatan (*firewall*) dan peralatan rangkaian hendaklah dapat menjana dan menyimpan log tindakan keselamatan atau jejak audit (*audit trail*).

g) Pematuhan

PKS KKDW hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk perlanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan maklumat.

h) Pemulihan

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

i) Saling Bergantungan

Setiap prinsip keselamatan adalah saling melengkapi dan bergantung antara satu dengan lain untuk membentuk sistem keselamatan maklumat ICT yang menyeluruh dan berkesan. Prinsip-prinsip ini tidak boleh dilaksanakan secara terpisah, tetapi mesti diintegrasikan dan diselaraskan untuk mencapai keselamatan yang maksimum dan menyeluruh.

#5

KAWALAN ORGANISASI *(ORGANIZATIONAL CONTROL)*



PKS KKDW V6

5 KAWALAN ORGANISASI (*ORGANIZATIONAL CONTROL*)

5.1 Polisi Keselamatan Siber (*Cyber Security Policy*)		
ID	**PENERANGAN**	**PERANAN**
5.1.1	**<u>Pelaksanaan Polisi (*Execution of the Policy*)</u>** Satu set polisi untuk keselamatan siber perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan Kementerian kepada pengguna, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT. Pelaksanaan polisi hendaklah dikuatkuasakan oleh Ketua Setiausaha dengan disokong oleh JPICT yang terdiri daripada Timbalan Ketua Setiausaha, Ketua Pegawai Digital (CDO) Kementerian, Setiausaha Bahagian, Ketua Unit, Ketua Agensi, Pengurus ICT Agensi, Ketua Pegawai Keselamatan ICT (ICTSO) dan ahli-ahli jemputan yang dilantik oleh Ketua Setiausaha.	Ketua Setiausaha
5.1.2	**<u>Pengesahan Polisi (*Endorsement of Policy*)</u>** Dasar itu perlu diperakui di peringkat JPICT Kementerian.	Ketua Setiausaha JPICT
5.1.3	**<u>Penguatkuasaan Polisi (*Enforcement of Policy*)</u>** PKS KKDW mestilah dipatuhi oleh semua warga Kementerian dan pihak luar yang mempunyai urusan berkaitan ICT Kementerian. Sebarang ketidakpatuhan kepada dasar ini boleh mengakibatkan tindakan tatatertib termasuk sebarang	Warga KKDW Pihak yang mempunyai urusan dengan perkhidmatan ICT di KKDW

	remedi/tindakan undang-undang lain di bawah akta/peraturan/undang-undang semasa yang berkuat kuasa.	
5.1.4	**<u>Penyebaran Polisi (*User Awareness*)</u>** Program kesedaran tentang polisi ini hendaklah diatur dan diselaraskan.	ICTSO
5.1.5	**<u>Pengecualian Polisi (*Exception to Policy*)</u>** Keselamatan ICT Kementerian adalah terpakai kepada semua warga Kementerian dan semua pihak yang terlibat dalam urusan ICT di Kementerian. Tiada sebarang pengecualian diberikan.	Warga KKDW Pihak yang terlibat dalam perkhidmatan ICT di KKDW
5.1.6	**<u>Penyelenggaraan Polisi (*Maintenance*)</u>** Penyelenggaraan dan kajian semula dasar hendaklah dilaksanakan mengikut keperluan. Semua dokumen atau rekod hendaklah diwujudkan dan diselenggarakan untuk menyediakan bukti pematuhan kepada keperluan dan operasi berkesan pengurusan keselamatan maklumat. Semua dokumen dan rekod hendaklah dilindungi dan dikawal mengikut undang-undang/arahan/peraturan/ garis panduan semasa yang berkuat kuasa.	CDO JPICT ICTSO
5.1.7	**<u>Kajian Semula/Semakan Polisi (*Policy Review*)</u>** Polisi ini perlu disemak dan dipinda pada jangka masa yang dirancang atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan, dan polisi	CDO JPICT ICTSO

	Kerajaan bagi memastikan kesesuaian, kecukupan dan keberkesanannya berterusan. Berikut ialah prosedur yang berkaitan dengan kajian semula Polisi Keselamatan Siber: g) Memastikan penguatkuasaan pelaksanaan Polisi ini; g) Mengenal pasti dan menentukan perubahan yang diperlukan; g) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan kepada JPICT bagi tujuan kelulusan; g) Memaklumkan pindaan yang telah disahkan oleh JPICT kepada warga Kementerian dan pihak yang mempunyai urusan dengan perkhidmatan ICT**;** dan g) Polisi ini hendaklah dikaji semula setiap **LIMA (5) TAHUN SEKALI** atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	
5.2 Peranan dan Tanggungjawab Keselamatan Maklumat (*Information Security Roles and Responsibilities*)		
ID	**PENERANGAN**	**PERANAN**
5.2.1	**<u>Peranan dan Tanggungjawab Keselamatan Maklumat (*The Role and Responsibility of Information Security*)</u>** Semua peranan dan tanggungjawab keselamatan maklumat hendaklah ditakrifkan dan diperuntukkan mengikut keperluan**.** **Objektif:** Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber KKDW.	

	Peranan dan Tanggungjawab Keselamatan Maklumat ialah seperti yang berikut:	
	a) Ketua Setiausaha i. Memastikan penguatkuasaan Polisi ini; ii. Memastikan warga dan pihak yang mempunyai urusan dengan perkhidmatan ICT memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini; iii. Memastikan semua keperluan seperti sumber kewangan, personel dan perlindungan keselamatan adalah mencukupi; iv. Memastikan pengurusan risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam Polisi ini; dan v. Melantik CDO dan ICTSO.	KSU
	b) Ketua Pegawai Digital (CDO) i. Memastikan polisi keselamatan siber selaras dengan matlamat digital jabatan dan mengurus risiko keselamatan dalam transformasi digital; ii. Membantu membangunkan, mengemas kini, dan melaksanakan PKS KKDW yang relevan dengan teknologi digital terkini; iii. Mendidik dan meningkatkan kesedaran keselamatan siber dalam kalangan warga KKDW serta memastikan penglibatan semua pihak berkepentingan; iv. Memastikan inisiatif digital mematuhi peraturan keselamatan siber dan mengawasi tadbir urus yang berkesan;	CDO

	v. Memastikan semua inisiatif digital dilaksanakan dengan selamat; vi. Menilai dan mengintegrasikan keselamatan dalam penggunaan teknologi digital baru tanpa menjejaskan inovasi; vii. Membantu dalam persediaan dan tindak balas terhadap insiden keselamatan siber, serta menilai keberkesanan selepas insiden berlaku; dan viii. Memastikan perlindungan data dan privasi dalam semua inisiatif digital, mematuhi peraturan yang berkaitan.	
	c) Pegawai Keselamatan ICT (ICTSO) i. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini; ii. Merangka pengurusan risiko dan audit keselamatan siber berpandukan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat yang berkuat kuasa; iii. Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlakunya ancaman keselamatan siber dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; iv. Melaporkan Insiden Keselamatan Siber kepada Pusat Kawalan dan Penyelarasan Siber Nasional (NC4) seterusnya membantu dalam penyiasatan atau pemulihan; v. Melaporkan Insiden Keselamatan Siber kepada Ketua Setiausaha bagi insiden yang memerlukan	ICTSO

	pengaktifan Pengurusan Kesinambungan Perkhidmatan (PKP); vi. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau Insiden Keselamatan Siber; vii. Memperakukan langkah-langkah baik pulih dengan segera; viii. Memastikan pematuhan Polisi ini oleh pengguna dan pihak yang mempunyai urusan dengan perkhidmatan ICT; ix. Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber; x. Menyedia dan merangka latihan dan program kesedaran keselamatan siber; xi. Merancang dan melaksanakan program kesedaran kepada semua warga untuk memahami keperluan standard, garis panduan dan prosedur keselamatan di bawah Polisi Keselamatan Siber ini; xii. Mewujudkan program-program bagi meningkatkan pengetahuan dan pembudayaan mengenai teknologi dan mekanisme kawalan maklumat dan aset ICT, ancaman-ancaman siber dan peranan dan tanggungjawab pengguna dalam mengendalikan kemudahan ICT; dan xiii. Mengurus keseluruhan program keselamatan ICT.	
	d) Setiausaha Bahagian/Ketua Unit/Pengarah PKN Peranan dan tanggungjawab Setiausaha Bahagian / Ketua Unit / Pengarah PKN ialah melaksanakan	Setiausaha Bahagian Ketua Unit Pengarah PKN

	keperluan Polisi ini dalam operasi semasa seperti yang berikut: i. Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu; ii. Menentukan pembekal dan rakan usaha sama menjalani tapisan keselamatan; dan iii. Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan dan pelan pengurusan keselamatan maklumat kerajaan yang sedang berkuat kuasa.	
	e) Pentadbir Sistem Pentadbir Sistem terdiri daripada: i. Pentadbir Rangkaian; ii. Pentadbir Keselamatan; iii. Pentadbir Portal (*Web Master*); iv. Pentadbir Pusat Data; v. Pentadbir Sistem Aplikasi; vi. Pentadbir E-mel; vii. Pentadbir Media Sosial dan Aplikasi Sosial KKDW; dan viii. Pegawai Aset ICT. **Tanggungjawab:** i. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai personel yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; ii. Menentukan ketepatan dan kesahihan sesuatu tahap capaian berdasarkan arahan pemilik	Pentadbir Sistem

	sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi ini; iii. Memantau aktiviti capaian sistem aplikasi; iv. Mengenal pasti dan melaporkan aktiviti-aktiviti tidak normal seperti pencerobohan atau pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta; v. Menganalisis dan menyimpan rekod jejak audit; vi. Menyediakan laporan mengenai aktiviti capaian secara berkala; dan vii. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada personel dalam keadaan yang baik.	
	f) Pemilik Sistem Sesuatu sistem hendaklah dimiliki oleh sesuatu Bahagian/Unit yang mempunyai kepentingan terhadap sistem yang dibangunkan. Peranan dan tanggungjawab Pemilik Sistem adalah seperti berikut: i. Pelaksanaan promosi sistem kepada pengguna sasaran; ii. Penentuan pengguna dan kategori atau tahap capaian pengguna sistem; iii. Pengurusan senarai pengguna yang terlibat di dalam Latihan Pengguna; iv. Penguatkuasaan penggunaan sistem di kalangan pengguna; v. Pemantauan pelaksanaan dan keberkesanan sistem secara berterusan; dan	Pemilik Sistem

	vi. Pemakluman sebarang masalah dan keperluan peningkatan sistem kepada Pembangun Sistem. Pemilik Sistem hendaklah melantik seorang pegawai sebagai Pentadbir Sistem untuk tujuan penyelenggaraan/ penambahbaikan sistem yang dikendalikan tersebut.	
	g) Jawatankuasa Pemandu ICT (JPICT) Peranan dan tanggungjawab JPICT seperti yang terkandung dalam **Surat Pekeliling Am Bil. 4 Tahun 2024: Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam** bagi pengurusan keselamatan siber.	JPICT
	h) *Cyber Security Incident Response Team* (CSIRT) Keanggotaan CSIRT adalah seperti berikut: **Pengarah**: Setiausaha Bahagian Kanan (Khidmat Pengurusan) / CDO **Pengurus**: Setiausaha Bahagian (ICT) **Ahli**: i. ICTSO Kementerian ii. Pegawai/ Penolong Pegawai Teknologi Maklumat Kementerian/ Agensi yang dilantik. Peranan dan tanggungjawab CSIRT adalah seperti yang berikut: i. Menerima dan mengesan aduan keselamatan siber serta menilai tahap dan jenis insiden;	CSIRT

	ii. Merekodkan dan menjalankan siasatan awal insiden yang diterima; iii. Menangani tindak balas insiden keselamatan siber dan mengambil tindakan baik pulih minimum; iv. Menasihati Pentadbir Sistem/Pelayan untuk mengambil tindakan pemulihan dan pengukuhan; dan v. Menyebarkan maklumat berkaitan pengukuhan keselamatan siber kepada Pentadbir Sistem ICT.	
	i) Pengguna/Warga i. Membaca, memahami dan mematuhi Polisi ini; ii. Mengetahui dan memahami implikasi keselamatan siber kesan daripada tindakannya; iii. Menjalani tapisan keselamatan sekiranya diperlukan dikehendaki berurusan dengan maklumat rasmi terperingkat; iv. Mematuhi prinsip-prinsip keselamatan Polisi ini dan menjaga kerahsiaan maklumat Kerajaan; v. Melaksanakan langkah-langkah perlindungan seperti yang berikut: • Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; • Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; • Menentukan maklumat sedia untuk digunakan; • Menjaga kerahsiaan maklumat;	Warga KKDW

	• Mematuhi dasar, piawaian dan garis panduan keselamatan siber yang ditetapkan; • Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan • Menjaga kerahsiaan kawalan keselamatan siber dari diketahui umum. vi. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada CSIRT Kementerian dengan segera; vii. Menghadiri program-program kesedaran mengenai keselamatan siber; dan viii. Bersetuju dengan terma dan syarat yang terkandung di dalam Polisi ini.	
5.3 Pengasingan Tugas (*Segregation of Duties*)		
ID	**PENERANGAN**	**PERANAN**
5.3.1	**<u>Pengasingan Tugas (*Segregation of Duties*)</u>** Pengasingan tugas dan bidang tanggungjawab dilaksanakan bagi mengurangkan peluang pengubahsuaian data dan maklumat tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah	Setiausaha Bahagian/ Ketua Unit KKDW/ Pengarah PKN

	diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; b) perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*; c) pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; d) pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya; dan e) Semakan dan pemantauan hak capaian perkakasan, perisian dan sistem hendaklah dilaksanakan secara berkala.	
5.4 Tanggungjawab Pengurusan (*Management Responsibilities*)		
ID	**PENERANGAN**	**PERANAN**
5.4.1	**<u>Tanggungjawab Pengurusan (*Management Responsibilities*)</u>** Pelaksanaan polisi ini akan dijalankan oleh Ketua Setiausaha dengan disokong oleh JPICT yang terdiri daripada Ketua Setiausaha, Timbalan Ketua Setiausaha, Ketua Pegawai Digital (CDO), Setiausaha Bahagian, Ketua Unit, Ketua Agensi, Pengurus ICT Agensi, Pegawai Keselamatan ICT (ICTSO) dan ahli-ahli yang dilantik oleh Ketua Setiausaha.	Setiausaha Bahagian/ Ketua Unit/Pengarah PKN

	Polisi Keselamatan Siber mestilah dipatuhi oleh semua pengguna dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian. Pengurusan hendaklah memastikan warga dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.	
5.5 Hubungan dengan Pihak Berkuasa (*Contact with Authorities*)		
ID	**PENERANGAN**	**PERANAN**
5.5.1	**<u>Hubungan dengan Pihak Berkuasa (*Contact with Authorities*)</u>** Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab; b) 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, penyedia perkhidmatan telekomunikasi dan perkhidmatan bekalan air;	Bahagian Pentadbiran dan Pengurusan Aset ICTSO CSIRT Pemilik Sistem

	c) insiden keselamatan maklumat harus dilaporkan tepat pada masanya ke pihak berkaitan seperti Agensi Keselamatan Siber (NACSA) selaras dengan Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022 bagi mengurangkan impak insiden; dan d) insiden keselamatan maklumat yang melibatkan NCII (*National Critical Information Infrastructure*) hendaklah dilaporkan dalam tempoh yang ditetapkan dalam Akta Keselamatan Siber 854 Peraturan-Peraturan Keselamatan Siber (Pemberitahuan Insiden Keselamatan Siber) 2024.	
5.6 Hubungan Dengan Kumpulan Berkepentingan Yang Khusus (*Contact with Special Interest Groups*)		
ID	**PENERANGAN**	**PERANAN**
5.6.1	**<u>Hubungan dengan Kumpulan Berkepentingan yang Khusus (*Contact with Special Interest Groups*)</u>** Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau pun forum bagi: a) meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat; b) memastikan pemahaman tentang persekitaran keselamatan maklumat adalah terkini; c) menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini;	CSIRT Pemilik Sistem

	d) mendapat akses kepada nasihat pakar keselamatan maklumat; e) berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan f) berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	
5.7 Perisikan Ancaman (*Threat Intelligence*)		
ID	**PENERANGAN**	**PERANAN**
5.7.1	**<u>Perisikan Ancaman (*Threat Intelligence*)</u>** Maklumat berkaitan ancaman keselamatan maklumat perlu diperoleh dan dianalisis untuk menghasilkan *threat intelligence* (perisikan ancaman). Maklumat tentang ancaman sedia ada atau baharu akan di kumpul dan dianalisis untuk: a) memudahkan tindakan dan mengelakkan ancaman daripada mendatangkan kemudaratan kepada pengguna; dan b) mengurangkan kesan ancaman tersebut. Perisikan ancaman harus dianalisis dan kemudian digunakan: a) memudahkan tindakan dan mengelakkan ancaman daripada mendatangkan kemudaratan kepada pengguna; b) dengan melaksanakan proses untuk memasukkan maklumat yang di kumpul daripada sumber risikan ancaman ke dalam proses pengurusan risiko keselamatan maklumat organisasi;	CSIRT Pemilik Sistem

	c) sebagai input tambahan kepada kawalan pencegahan dan detektif teknikal seperti *Firewall*, Sistem Pengesanan Pencerobohan atau *Anti-Malware Solution*; dan d) sebagai input kepada proses dan teknik ujian keselamatan maklumat.	
5.8 Keselamatan Maklumat dalam Pengurusan Projek (*Information Security in Project Management*)		
ID	**PENERANGAN**	**PERANAN**
5.8.1	**<u>Keselamatan Maklumat dalam Pengurusan Projek (*Information Security in Project Management*)</u>** Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek tanpa mengira kerumitan, saiz, tempoh atau jenis aplikasinya. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek; b) objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek; c) pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan; d) kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam polisi keselamatan siber; e) penyediaan spesifikasi perolehan digalakkan memasukkan keperluan **pasukan projek pihak**	Pengarah Projek Pengurus Projek

	berkaitan yang mempunyai pensijilan keselamatan maklumat; f) kesesuaian pertimbangan dan aktiviti keselamatan maklumat hendaklah disusuli pada peringkat yang telah ditetapkan seperti Jawatankuasa Teknikal Projek, Jawatankuasa Pemandu Projek atau Jawatankuasa setara; dan g) peranan dan tanggungjawab keselamatan maklumat projek hendaklah ditakrif dan ditentukan.	
5.8.2	**<u>Analisis dan Spesifikasi Keperluan Keselamatan Maklumat (*Information Security Requirements Analysis and Specifications*)</u>** Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada dan hendaklah mematuhi perkara-perkara berikut: a) Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk pengkonsepan perisian, kajian keperluan, reka bentuk, pelaksanaan, pengujian, penerimaan, pemasangan, penyelenggaraan dan pelupusan; b) Semua sistem yang akan dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Polisi Keselamatan Siber; c) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan	Pentadbir Sistem

	d) Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data.	
5.9 Inventori Maklumat dan Aset Lain yang Berkaitan (*Inventory of Information and Other Associated Assets*)		
ID	**PENERANGAN**	**PERANAN**
5.9.1	**<u>Inventori Aset (*Inventory of Assets*)</u>** Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT Kementerian. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: a) Kementerian hendaklah mengenal pasti Pegawai Penerima Aset setiap Bahagian/ Unit untuk menguruskan penerimaan aset-aset ICT bagi projek-projek ICT; b) Memastikan semua aset ICT dikenal pasti, di klasifikasi, di dokumen, di selenggara dan dilupuskan. Maklumat aset di rekod dan dikemas kini sebagaimana arahan dan peraturan yang berkuat kuasa dari masa ke semasa; c) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; d) Memastikan inventori maklumat dan aset lain yang berkaitan hendaklah tepat, terkini, dan konsisten; e) Pegawai Aset hendaklah mengesahkan penempatan aset ICT; dan f) Memastikan inventori aset sewaan diurus mengikut kaedah yang bersesuaian yang ditetapkan.	Pegawai Aset Pegawai Penerima Aset

5.9.2	**<u>Pemilikan Aset (*Ownership of Assets*)</u>** Aset yang di selenggara hendaklah merupakan hak milik Kementerian. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara-perkara berikut: a) memastikan aset didaftarkan dalam senarai aset mengikut klasifikasi aset dan diserahkan kepada pemilik aset; b) memastikan semua jenis aset dipelihara dan di selenggara dengan baik; c) Kenal pasti dan kaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan; d) memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan e) aset bukan hak milik Kementerian hendaklah didaftarkan dan diurus mengikut prosedur/arahan-arahan yang berkuat kuasa.	Pegawai Aset Pengguna Aset
5.9.3	**<u>Pengelasan Maklumat Aset (*Information Classification Assets*)</u>** Memastikan setiap aset ICT diklasifikasikan mengikut klasifikasi aset.	Pegawai Pengelas

5.10 Penggunaan Maklumat yang Boleh Diterima dan Aset Lain yang Berkaitan (*Acceptable Use of Information and Other Associated Assets)*		
ID	**PENERANGAN**	**PERANAN**
5.10.1	**<u>Penggunaan Aset yang Dibenarkan (*Acceptable Use of Assets*)</u>** Memastikan pengguna menggunakan aset ICT untuk tujuan rasmi dan mengikut fungsi sebenar yang telah ditetapkan oleh Kementerian.	Pengguna Aset
5.10.2	**<u>Pengendalian Aset (*Handling of Assets*)</u>** Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah perlu mengambil kira langkah-langkah keselamatan berikut: a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa dan menentukan maklumat adalah tepat dan lengkap dari semasa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan; e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, membuat salinan, penghantaran, penyampaian, pertukaran dan pemusnahan; g) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum; h) Sekatan akses yang menyokong keperluan perlindungan untuk setiap peringkat pengelasan;	Pegawai Aset Pengguna Aset

	i) Penyelenggaraan rekod pengguna yang dibenarkan bagi maklumat dan aset lain yang berkaitan; dan j) Memastikan perkara a) hingga i) juga terpakai kepada aset sewaan.	

5.11 Pemulangan Aset (*Return of Assets*)		
ID	**PENERANGAN**	**PERANAN**
5.11.1	**<u>Pemulangan Aset (*Return of Assets*)</u>** Pengguna perlu mengembalikan aset termasuk semua aset lain yang berkaitan seperti peranti storan mudah alih, peranti pengguna fizikal yang disambungkan kepada sistem rangkaian, salinan maklumat fizikal dan perkakasan pengesahan (cth. kunci mekanikal, token fizikal dan kad pintar) untuk sistem maklumat, tapak serta arkib fizikal mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar Kementerian atau penamatan perkhidmatan atau kontrak. Pemulangan aset-aset yang dipinjam atau disewakan hendaklah di sanitasi mengikut Surat Pekeliling Am Bil.4 Tahun 2022 Garis Panduan Sanitasi Media Elektronik dalam Perkhidmatan Awam.	Pegawai Aset Pengguna Aset

5.12 Pengelasan Maklumat (*Classification of Information*)		
ID	**PENERANGAN**	**PERANAN**
5.12.1	**<u>Pengelasan Maklumat (*Classification of Information*)</u>** Data dan maklumat perlu di kelas oleh Pegawai Pengelas mengikut keperluan keselamatan maklumat yang telah ditetapkan di dalam Arahan Keselamatan berdasarkan	Pegawai Rekod Pegawai Pengelas Pegawai Pengurus Rekod

	kerahsiaan, integriti, ketersediaan/kebolehsediaan dan keperluan pihak berkepentingan lain. Klasifikasi dan kawalan perlindungan maklumat yang berkaitan hendaklah mengambil kira keperluan perkhidmatan untuk berkongsi atau menyekat maklumat, untuk melindungi kerahsiaan, integriti atau ketersediaan maklumat. Aset selain daripada maklumat boleh diklasifikasikan mengikut klasifikasi maklumat, yang disimpan dalam, diproses oleh atau sebaliknya dikendalikan atau dilindungi oleh aset harus mengambil kira keperluan untuk kerahsiaan, integriti dan ketersediaan dalam skim pengelasan. a) Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditandai dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan. b) Patuhi piawaian, prosedur, tatacara dan garis panduan keselamatan yang dikeluarkan. c) Memberi perhatian semasa mengendalikan maklumat rahsia terperingkat. d) Elak pendedahan maklumat kepada pihak yang tidak dibenarkan. e) Pengelasan maklumat adalah berpandukan kepada Arahan Keselamatan, Arkib negara, Akta Rahsia Rasmi 1972 dan Surat Pekeliling Am Bil.2/1987 Peraturan Pengelasan Semula Rekod Terperingkat. f) Fail Satu folder yang diklasifikasikan mengikut kaedah yang tertentu (nombor/abjad dan sebagainya) supaya kandungan di dalamnya mudah dikesan. g) Kategori fail:	

	i. Fail Rahsia Besar adalah fail berwarna kuning dengan berpalang merah di sebelah luar kulit hadapan dan belakang - disimpan dalam bilik kebal atau peti besi yang seelok-eloknya dipasang dengan kunci tata kira; ii. Fail Rahsia adalah fail berwarna merah jambu dengan berpalang merah di sebelah luar kulit hadapan dan belakang - disimpan sama seperti dokumen terperingkat RAHSIA BESAR atau dalam kabinet keluli atau almari keluli yang dipasang dengan palang besi berkunci; iii. Fail Rasmi adalah dokumen rasmi kerajaan yang dikandung, disusun dengan teratur dan didaftarkan. Fail ini diberi tajuk spesifik sepertimana yang telah ditetapkan dalam Klasifikasi Fail; iv. Fail Sulit adalah fail berwarna hijau - disimpan dalam kabinet keluli atau almari keluli; v. Fail Terhad adalah fail berwarna putih - disimpan dalam kabinet keluli atau almari keluli; dan vi. Fail Terbuka adalah fail berwarna putih - disimpan dalam kabinet keluli atau almari keluli.	
5.13 Pelabelan Maklumat (*Labelling of Information*)		
ID	**PENERANGAN**	**PERANAN**
5.13.1	**<u>Pelabelan Maklumat (*Labelling of Information*)</u>** Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan. a) Memastikan setiap maklumat diberikan tahap perlindungan yang bersesuaian.	Pegawai Rekod Pegawai Pengelas Pegawai Pengurus Rekod

	b) Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut Arkib Negara.	
5.14 Pemindahan Data dan Maklumat (*Information Transfer*)		
ID	**PENERANGAN**	**PERANAN**
5.14.1	**<u>Polisi dan Prosedur Pemindahan Data dan Maklumat (*Information Transfer Policies and Procedures*)</u>** Memastikan keselamatan perpindahan/pertukaran data, maklumat dan perisian antara dan pihak luar terjamin dengan merujuk pada Dasar Perkongsian Data Sektor Awam dan Dasar Perkongsian Data Nasional. Pihak luar ialah pihak yang menggunakan atau pihak yang membekalkan data, maklumat atau perisian. Perkara yang perlu dipatuhi ialah seperti yang berikut: a) Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; b) Terma pemindahan data, maklumat dan perisian antara jabatan dengan pihak luar hendaklah dimasukkan di dalam Perjanjian; c) Media yang mengandungi maklumat perlu dilindungi; dan d) Memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.	Pemilik Sistem Pentadbir Sistem

5.14.2	**<u>Perjanjian Mengenai Pemindahan Data dan Maklumat (*Agreements on Information Transfer*)</u>** Semua pihak yang terlibat perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara Kementerian dengan pihak luar. Perkara yang perlu dipertimbangkan ialah: a) Setiausaha Bahagian/ Ketua Unit/ Pengarah PKN hendaklah mengawal penghantaran dan penerimaan maklumat Kementerian; b) Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat Kementerian; c) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; d) hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data; dan e) merujuk dan patuh Dasar Perkongsian Data Sektor Awam dan Dasar Perkongsian Data Nasional.	Setiausaha Bahagian / Ketua Unit/ Pengarah PKN Pemilik Sistem Warga KKDW
5.14.3	**<u>Pesanan Elektronik (*Electronic Messaging*)</u>** Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan, peraturan dan garis panduan yang sedang berkuat kuasa bagi pengurusan pesanan elektronik.	Warga KKDW

5.15 Kawalan Capaian (*Access control*)		
ID	**PENERANGAN**	**PERANAN**
5.15.1	**<u>Polisi Kawalan Akses (*Access Control Policy*)</u>** Dasar khusus mengenai kawalan akses hendaklah ditakrifkan dengan mengambil kira keperluan ini dan harus dimaklumkan kepada semua pihak yang berkepentingan yang berkaitan. Pemilik Sistem dan pemilik aset hendaklah menentukan tahap perlindungan keselamatan maklumat dan kawalan capaian yang diperlukan bagi mencapai maklumat tersebut. Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Kawalan akses ditetapkan berdasar prinsip perlu tahu iaitu capaian diberikan akses atas dasar keperluan untuk melaksanakan tugas dan keperluan untuk digunakan (hanya diberikan akses kepada infrastruktur teknologi maklumat di mana terdapat keperluan yang jelas). Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu disemak, dikemas kini dan disahkan sekurang-kurangnya sekali dalam tempoh setahun atau mengikut keperluan serta menyokong peraturan kawalan capaian pengguna sedia ada. Perkara-perkara yang perlu dipertimbangkan dalam menentukan kawalan akses adalah seperti berikut:	Pentadbir Sistem Pemilik Sistem

	a) Menentukan entiti mana yang memerlukan jenis akses kepada maklumat dan aset lain yang berkaitan; b) keperluan keselamatan aplikasi ditentukan dan diselaraskan dengan keperluan akses entiti; c) Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian; d) Akses fizikal, yang perlu disokong oleh kawalan kemasukan fizikal yang sesuai; e) Penyebaran maklumat dan kebenaran capaian mematuhi prinsip-prinsip keselamatan yang ditetapkan dan mengikut tahap keselamatan maklumat serta klasifikasi maklumat yang dibenarkan; f) Sekatan kepada akses istimewa hendaklah dihadkan dan diuruskan dengan baik (pengurusan hak akses); g) Pengasingan tugas, fungsi kawalan capaian. Contohnya, permintaan capaian, kebenaran capaian, dan pentadbiran capaian; h) Patuh undang-undang, peraturan berkaitan yang sedang berkuat kuasa dan sebarang kewajipan kontrak berkaitan pengehadan akses kepada data atau perkhidmatan; i) Kebenaran rasmi untuk permintaan akses; j) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; k) Pengasingan peranan kawalan capaian; l) Kebenaran rasmi permohonan akses; m) Keperluan semakan hak akses berkala; n) Pembatalan hak akses;	

	o) Pengarkiban semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; p) Hak capaian istimewa; dan q) Log setiap aktiviti yang terlibat.	
5.15.2	**<u>Capaian kepada Rangkaian dan Perkhidmatan Rangkaian (*Access to Networks and Network Services*)</u>** Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari Kementerian. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Menempatkan atau memasang perkakasan ICT yang bersesuaian antara rangkaian Kementerian, rangkaian kementerian / jabatan / agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pentadbir Sistem Pentadbir Rangkaian
5.15.3	**<u>Kawalan Capaian Maklumat (*Information Access Control*)</u>** Kawalan capaian adalah untuk menguruskan, mengawasi, dan meningkatkan capaian maklumat dan aset dengan selamat. Ini merangkumi pelbagai aspek operasi dan pengurusan untuk memastikan mencapai matlamat, sasaran, dan hasil yang diinginkan dengan kawalan seperti berikut:	Bahagian Pentadbiran dan Pengurusan Aset Bahagian Pengurusan Maklumat

	a) Mematuhi undang-undang, peraturan, dan polisi yang berkaitan dengan keselamatan maklumat; b) Memastikan bahawa dasar, prosedur, dan amalan keselamatan maklumat diikuti dan dilaksanakan dengan betul; c) Mengenal pasti, menilai, dan menguruskan risiko keselamatan maklumat yang berkaitan dengan operasi dan capaian maklumat organisasi; d) Memastikan keselamatan maklumat dan data dalam organisasi dengan mematuhi amalan keselamatan maklumat yang sesuai; e) Meningkatkan kesedaran dan kefahaman kakitangan tentang peningkatan capaian dan amalan keselamatan dalam organisasi; dan f) Memantau dan menilai prestasi keselamatan capaian berterusan untuk mengenal pasti peningkatan dan kesan tindakan yang diperlukan.	
5.15.4	**<u>Keperluan Perkhidmatan Kawalan Akses (*Service Requirements of Access Control*)</u>** Mengehadkan akses pembekal, kakitangan dan pengguna pihak luar kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat. Memastikan prosedur kawalan akses dengan pihak ketiga dipatuhi.	ICTSO Pemilik Sistem Pentadbir Sistem Warga KKDW Pihak yang mempunyai urusan dengan perkhidmatan ICT di KKDW

5.16 Pengurusan Identiti (*Identity Management*)		
ID	**PENERANGAN**	**PERANAN**
5.16.1	**<u>Pendaftaran dan Pembatalan Pengguna (*User Registration and De-Registration*)</u>** Setiap pengguna adalah bertanggungjawab ke atas aset maklumat yang diamanahkan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: a) Akaun pengguna hanya diwujudkan setelah mendapat pengesahan Bahagian Pengurusan Maklumat dan pengguna telah mengesahkan memahami PKS KKDW seperti di **Lampiran A: Akuan Pematuhan Polisi Keselamatan Siber;** b) Akaun yang diperuntukkan sahaja boleh digunakan; c) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; d) Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada Pemilik Sistem terlebih dahulu; e) Sebarang perubahan tahap akses hendaklah mendapat pengesahan daripada penyelia/Ketua Jabatan terlebih dahulu; f) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan penyelia/Ketua Jabatan; g) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan. h) Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;	Warga KKDW Pengguna Aset Pentadbir Sistem

	i) Penggunaan akaun milik individu lain adalah **DILARANG**; j) Akaun pengguna tidak boleh dikongsi; k) Akaun pengguna boleh dibekukan atau ditamatkan apabila menerima arahan daripada Bahagian Pengurusan Sumber Manusia atas sebab-sebab berikut: i. Pengguna bercuti panjang dalam tempoh waktu melebihi tiga (3) minggu; ii. Bertukar bidang tugas kerja; iii. Bertukar ke jabatan lain; iv. Bersara; v. Bagi menjalankan siasatan; atau vi. Ditamatkan perkhidmatan. l) Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. la perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	
5.16.2	**<u>Pengurusan Identiti (*Identity Management*)</u>** Menguruskan *profiling* kakitangan bermula daripada penciptaan rekod kakitangan baharu sehingga penamatan profil apabila kakitangan meninggalkan pekerjaan (pencen, berhenti kerja atau kematian) serta kawalan capaian pengguna ke atas aset ICT. Pendaftaran, pengemaskinian dan penamatan akaun pengguna dilaksanakan mengikut prosedur yang ditetapkan.	Warga KKDW Pentadbir Sistem

	Proses pengurusan identiti harus memastikan bahawa: a) Identiti yang diberikan khusus hanya dikaitkan dengan seorang sahaja untuk membolehkan orang itu bertanggungjawab atas tindakan yang dilakukan dengan identiti khusus ini; b) Identiti yang diberikan kepada berbilang orang (contoh: identiti bersama, *mail group*) hanya dibenarkan bagi keperluan atas sebab perkhidmatan atau operasi sahaja; c) identiti yang diberikan kepada entiti bukan manusia seperti mesin atau sistem tertakluk kepada kelulusan yang diasingkan dengan sewajarnya dan pengawasan berterusan; d) akaun pengguna perlu dinyahaktifkan dengan segera jika tidak lagi diperlukan; e) dalam domain tertentu, identiti tunggal dihubungkan dengan entiti tunggal; dan f) rekod penggunaan dan pengurusan identiti pengguna dan maklumat pengesahan hendaklah disimpan.	
5.17 Maklumat Pengesahan (*Authentication Information*)		
ID	**PENERANGAN**	**PERANAN**
5.17.1	**<u>Pengurusan Maklumat Pengesahan Identiti Pengguna (*Management of Secret Authentication Information*)</u>** Peruntukan maklumat pengesahan identiti pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan. Peruntukan dan proses pengurusan hendaklah memastikan bahawa:	Warga KKDW Pentadbir Sistem

	a) Kata laluan peribadi atau nombor pengenalan diri (PIN) yang dijana secara automatik semasa proses pendaftaran sebagai maklumat pengesahan rahsia sementara adalah tidak dapat tidak dapat diteka dan unik untuk setiap orang, dan pengguna dikehendaki menukarnya selepas penggunaan pertama; b) Prosedur yang telah diwujudkan untuk mengesahkan identiti pengguna sebelum memberikan maklumat pengesahan baru, gantian atau sementara; c) Maklumat pengesahan, termasuk maklumat pengesahan sementara, dihantar kepada pengguna secara selamat (contohnya, melalui saluran yang disahkan dan dilindungi), dan penggunaan mesej e-mel elektronik yang tidak dilindungi (*clear text*) untuk tujuan ini dielakkan; d) Pengguna mengakui penerimaan maklumat pengesahan identiti pengguna; e) Maklumat pengesahan tetapan asal (*default*) seperti yang ditetapkan atau diberikan diubah dengan segera selepas pemasangan sistem atau perisian; dan f) Rekod peristiwa penting mengenai peruntukan dan pengurusan maklumat pengesahan identiti pengguna disimpan dan kerahsiaannya dijamin, serta kaedah penyimpanan rekod disetujui (contohnya, dengan menggunakan alat penyimpanan kata laluan yang diluluskan).	

5.17.2	**<u>Penggunaan Maklumat Pengesahan Rahsia (*Use of Secret Authentication Information*)</u>** Peranan dan tanggungjawab pengguna adalah seperti yang berikut: a) Membaca, memahami dan mematuhi PKS KKDW; b) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya; c) Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat organisasi; d) Melaksanakan langkah-langkah perlindungan seperti yang berikut: • Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; • Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; • Menentukan maklumat sedia untuk digunakan; • Menjaga kerahsiaan kata laluan; • Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; • Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; • Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum; • maklumat pengesahan terjejas atau telah di kompromi hendaklah diubah serta-merta apabila pemberitahuan atau petunjuk sebarang kompromi diterima; • Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera; dan	Warga KKDW Pentadbir Sistem

	• Menghadiri program-program kesedaran mengenai keselamatan siber. Pengguna perlu mengikut amalan keselamatan yang baik dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti.	
5.17.3	**<u>Sistem Pengurusan Kata Laluan (*Password Management System*)</u>** Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh KKDW seperti yang berikut: a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau di kompromi. Kata laluan di cadang untuk ditukar sekurang-kurangnya sekali dalam tempoh tiga bulan; c) Panjang kata laluan mestilah sekurang kurangnya **<u>DUA BELAS (12) AKSARA</u>** dengan gabungan antara huruf, aksara khas dan nombor (*alphanumeric*) **<u>KECUALI</u>** bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad; d) Kata laluan hendaklah diingat dan **<u>TIDAK BOLEH</u>** dicatat, disimpan atau didedahkan dengan apa cara sekali pun; e) Kata laluan paparan kunci (*lock screen*) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;	Warga KKDW Pentadbir Sistem

	f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara; g) Kuat kuasakan pertukaran kata laluan semasa atau selepas *login* kali pertama atau selepas *reset* kata laluan; h) kata laluan tidak berdasarkan perkataan kamus atau gabungannya; i) kata laluan yang sama tidak digunakan merentas perkhidmatan dan sistem yang berbeza; j) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; k) Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum **TIGA (3) KALI** sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; dan l) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	

5.18 Hak Capaian (*Access Rights*)		
ID	**PENERANGAN**	**PERANAN**
5.18.1	**Peruntukan Akses Pengguna (*User Access Provisioning*)** Hak akses kepada maklumat dan aset yang berkaitan hendaklah diperuntukkan, disemak, diubah suai dan dikeluarkan mengikut dasar/ peraturan atau garis panduan kawalan akses yang berkuat kuasa. Pentadbir Sistem ICT perlu mewujudkan Prosedur Pendaftaran dan Penamatan Pengguna sistem masing-masing.	Pentadbir Sistem Pihak yang mempunyai urusan dengan perkhidmatan ICT di KKDW

	Proses peruntukan akses pengguna dan pembatalan hak akses fizikal dan logik yang diberikan kepada entiti yang telah disahkan identitinya hendaklah termasuk; a) Hak Akses yang berkaitan dengan setiap sistem atau produk yang perlu diberikan hendaklah dikenal pasti dan dibenarkan; b) Hak akses maklumat dan aset mesti dihadkan berdasarkan keperluan untuk mengetahui dan prinsip-prinsip keselamatan yang ditetapkan; c) Individu yang bukan warga KKDW **TIDAK BOLEH** diberikan ID pengguna atau diberi keistimewaan untuk menggunakan atau mengakses aset (komputer, maklumat atau sistem komunikasi) melainkan ia dibenarkan; d) Kebenaran rasmi mestilah telah ditandatangani oleh wakil yang diberi kuasa di organisasi pihak ketiga sebelum akses diberikan kepada mana-mana pihak ketiga; e) Hak akses hendaklah ditamatkan apabila entiti/ individu tidak lagi perlu mengakses maklumat dan aset yang berkaitan tepat pada masanya; f) Hak akses sementara untuk tempoh masa terhad boleh dipertimbangkan bila diperlukan dan hendaklah dibatalkan selepas tamat tempoh; g) Tahap akses yang diberikan hendaklah mengikut dasar kawalan akses yang ditetapkan, peranan dan konsisten dengan keperluan keselamatan maklumat lain seperti pengasingan tugas; h) Hak akses pengguna hendaklah diubah suai selari dengan peranan atau pekerjaan; i) Hak akses diaktifkan hanya selepas kebenaran diperoleh; dan	

	j) Rekod hak akses logik dan fizikal pengguna hendaklah disimpan.	
5.18.2	**<u>Kajian Semula Hak Akses Pengguna (*Review of User Access Rights*)</u>** Pemilik aset hendaklah menyemak hak akses pengguna secara berkala atau mengikut keperluan dan dicadangkan sekurang-kurangnya sekali dalam tempoh setahun. Pentadbir Sistem perlu mewujudkan Rekod Pendaftaran dan Penamatan Pengguna sistem masing-masing sebagai rujukan semakan ke atas hak akses pengguna secara berkala. Semakan ke atas hak akses fizikal dan logik harus mempertimbangkan perkara berikut: a) Hak akses pengguna selepas sebarang perubahan dalam organisasi (contoh: pertukaran pekerjaan, kenaikan pangkat, penurunan pangkat) atau penamatan perkhidmatan/ pekerjaan; dan b) Kebenaran untuk hak akses istimewa.	Pentadbir Sistem Pihak yang mempunyai urusan dengan perkhidmatan ICT di KKDW
5.18.3	**<u>Pembatalan atau Pelarasan Hak Akses (*Removal or Adjustment of Access Rights*)</u>** Hak akses pengguna kepada maklumat dan aset yang berkaitan hendaklah disemak dan diselaraskan atau ditamatkan sebelum sebarang perubahan atau penamatan pekerjaan berdasarkan penilaian faktor risiko seperti:	Pentadbir Sistem Pihak yang mempunyai urusan dengan perkhidmatan ICT di KKDW

	a) Sama ada penamatan atau perubahan penempatan oleh pengguna atau pengurusan dan sebab penamatan; b) Tanggungjawab semasa pengguna; dan c) Nilai semasa aset yang boleh diakses oleh pengguna. 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 organisasi.	
5.18.4	**<u>Tanggungjawab Pengguna (*User Responsibilities*)</u>** Memastikan pengguna sistem atau aset maklumat bertanggungjawab melindungi maklumat pengesahan mereka.	Warga KKDW Pihak yang mempunyai urusan dengan perkhidmatan ICT di KKDW
5.19 Keselamatan Maklumat Dalam Hubungan Pembekal (*Information Security in Supplier Relationships*)		
ID	**PENERANGAN**	**PERANAN**
5.19.1	**<u>Keselamatan Maklumat dalam Hubungan Pembekal (*Information Security in Supplier Relationships*)</u>** Keperluan keselamatan maklumat hendaklah ditakrifkan, dilaksanakan, dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset maklumat. Perkara yang dipertimbangkan ialah seperti yang berikut:	Pengurus Projek Pembekal Pihak yang mempunyai urusan dengan

	a) Mengenal pasti dan mendokumenkan maklumat pembekal; b) Menyediakan prosedur pengurusan pembekal termasuk kaedah penilaian mutu perkhidmatan; c) Memilih perkhidmatan yang disediakan oleh pembekal selaras dengan dasar dan peraturan yang berkuat kuasa; d) Mengawal dan memantau akses pembekal; e) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam dokumen perjanjian; f) Jenis-jenis obligasi kepada pembekal; g) Pelan kontingensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat; h) Melaksanakan program kesedaran Polisi Keselamatan Siber KKDW kepada pembekal; i) Menandatangani Surat Setuju Terima, dan akuan pematuhan Polisi Keselamatan Siber KKDW; j) Pembekal perlu mematuhi arahan keselamatan yang sedang berkuat kuasa; dan k) Mengenal pasti dan melaksanakan proses dan prosedur bagi mengurus risiko yang berkaitan dengan penggunaan produk dan perkhidmatan pembekal termasuk penamatan penggunaan produk dan perkhidmatan pembekal. Pemilik perkhidmatan atau projek hendaklah memastikan proses penamatan pembekal yang selamat, termasuk: a) membatalkan peruntukan hak akses; b) pengendalian maklumat;	perkhidmatan ICT di KKDW ICTSO

	c) menentukan pemilikan harta intelek yang dibangunkan semasa perjanjian dilaksanakan; d) mudah alih maklumat sekiranya berlaku pertukaran pembekal atau penyumberan; e) pengurusan rekod; f) pemulangan aset; g) pelupusan selamat maklumat dan aset lain yang berkaitan; dan h) keperluan kerahsiaan berterusan.	
5.20 Menangani Keselamatan dalam Perjanjian dengan Pembekal (*Addressing Security within Supplier Agreements*)		
ID	**PENERANGAN**	**PERANAN**
5.20.1	**<u>Menangani Keselamatan dalam Perjanjian dengan Pembekal (*Addressing Security within Supplier Agreements*)</u>** Semua keperluan keselamatan maklumat yang berkaitan hendaklah ditakrifkan, 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 Kementerian selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa. Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal	Pengurus Projek Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT di KKDW

	daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Kementerian hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan; b) Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan; c) Semua wakil syarikat pembekal mempunyai kelulusan keselamatan daripada jabatan berkaitan; d) Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; e) Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal; f) Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti berikut: i. Badan penilai pihak ketiga adalah bebas dan berintegriti; ii. Badan penilai pihak ketiga adalah kompeten; iii. Kriteria penilaian; iv. Parameter pengujian; dan v. Andaian yang dibuat berkaitan dengan skop penilaian. g) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang	

	relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan jabatan dan Perakuan Akta Rahsia Rasmi 1972 (Akta 88); dan h) Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh Kementerian.	
5.21 Menguruskan Keselamatan Maklumat dalam Rantaian Bekalan Teknologi Maklumat dan Komunikasi (*Managing Information Security in The Information and Communication Technology (ICT) Supply Chain*)		
ID	**PENERANGAN**	**PERANAN**
5.21.1	**<u>Rantaian Bekalan Teknologi Maklumat dan Komunikasi (*Information and Communication Technology Supply Chain*)</u>** Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian 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	Pengurus Projek

	c) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	
5.22 Memantau, Menyemak dan Mengubah Pengurusan Perkhidmatan Pembekal (*Monitoring, Review and Change Management of Supplier Services*)		
ID	**PENERANGAN**	**PERANAN**
5.22.1	**<u>Memantau dan Mengkaji Semula Perkhidmatan Pembekal (*Monitoring and Review Supplier Services*)</u>** Kementerian hendaklah sentiasa memantau, mengkaji semula, mengaudit perkhidmatan pembekal secara berkala dan mengurus perubahan dalam amalan risiko keselamatan maklumat pembekal dan penyampaian perkhidmatan. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan c) Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek sekiranya berkaitan.	Pengurus Projek

5.22.2	**<u>Menguruskan Perubahan Kepada Perkhidmatan Pembekal (*Managing Changes to Supplier Services*)</u>** Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahan 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: a) Perubahan dalam perjanjian dengan pembekal; b) Perubahan yang dilakukan oleh jabatan bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan subkontraktor.	Pengurus Projek

5.23 Keselamatan Maklumat bagi Penggunaan Perkhidmatan Awan (*Information Security for Use of Cloud Services*)		
ID	**PENERANGAN**	**PERANAN**
5.23.1	**<u>Keselamatan Maklumat bagi Penggunaan Perkhidmatan Awan (*Information Security for Use of Cloud Services*)</u>** Pengurusan perkhidmatan awan ini melibatkan pelbagai aspek teknikal dan pentadbiran untuk memastikan perkhidmatan awan digunakan secara berkesan, selamat dan sesuai dengan keperluan organisasi.	Pentadbir Perkhidmatan Pengkomputeran Awan Pentadbir Sistem

	Perkara berikut perlu dipatuhi oleh semua pihak yang terlibat: a) Memastikan kepatuhan terhadap keperluan perundangan, peraturan, garis panduan dan perjanjian kontrak yang sedang berkuat kuasa dan Pengurusan perkhidmatan yang disediakan oleh pembekal seperti di 5.21 dan 5.22; b) Menentukan/mentakrifkan dan memaklumkan cara/kaedah berkaitan pengurusan risiko bagi perkhidmatan pengkomputeran awan; c) Memastikan keperluan keselamatan maklumat yang berkaitan dengan penggunaan perkhidmatan pengkomputeran awan dilaksanakan; dan d) Melaksanakan kawalan terhadap keperluan pelesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	
5.24 Perancangan dan Penyediaan Pengurusan Insiden Keselamatan Maklumat (*Information Security Incident Management Planning and Preparation*)		
ID	**PENERANGAN**	**PERANAN**
5.24.1	**<u>Tanggungjawab dan Prosedur (*Responsibilities and Procedures*)</u>** Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat dengan mentakrif, mewujudkan dan menyampaikan proses pengurusan insiden keselamatan maklumat, peranan dan tanggungjawab. Pengurusan insiden Kementerian adalah berdasarkan kepada pengurusan insiden keselamatan ICT yang	ICTSO CSIRT Pemilik Sistem

	sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Memberikan kesedaran keselamatan ICT dan hebahan kepada warga Kementerian sekiranya ada perubahan; b) Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan; dan c) Mematuhi Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022.	
5.24.2	**<u>Perancangan dan Penyediaan Pengurusan Insiden Keselamatan Maklumat (*Information Security Incident Management Planning and Preparation*)</u>** Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi tentang kejadian dan kerentanan kelemahan keselamatan.	ICTSO CSIRT Pemilik Sistem
5.25 Penilaian dan Keputusan mengenai Kejadian Keselamatan Maklumat (*Assessment of and Decision on Information Security Events*)		
ID	**PENERANGAN**	**PERANAN**
5.25.1	**<u>Penilaian dan Keputusan Mengenai Peristiwa Keselamatan Maklumat (*Assessment of and Decision on Information Security Events*)</u>** Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat dan hendaklah direkodkan sebagaimana pekeliling Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam.	ICTSO Pemilik sistem CSIRT

5.26 Tindak Balas Terhadap Insiden Keselamatan Maklumat (*Response to Information Security Incidents*)		
ID	**PENERANGAN**	**PERANAN**
5.26.1	**<u>Tindak Balas Terhadap Insiden Keselamatan Maklumat (*Response to Information Security Incidents*)</u>** Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan kepada Pekeliling Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut: a) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; b) Menjalankan kajian forensik sekiranya perlu; c) Menghubungi pihak yang berkenaan dengan secepat mungkin; d) Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti; e) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; f) Menyediakan pelan kontingensi dan mengaktifkan Pelan Pemulihan Bencana (DRP) atau Pelan Kesinambungan Perkhidmatan sekiranya perlu; g) Menyediakan tindakan pemulihan segera; h) Memaklumkan atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu;	ICTSO Pemilik Sistem CSIRT

	i) sebaik sahaja insiden itu berjaya ditangani, ia hendaklah ditutup secara rasmi dan direkodkan; j) melaksanakan analisis pasca-kejadian untuk mengenal pasti punca asal. Pastikan ia didokumentasikan mengikut prosedur yang ditakrifkan; dan k) mengenal pasti dan mengurus kelemahan dan kelemahan keselamatan maklumat termasuk yang berkaitan dengan kawalan yang telah menyebabkan, menyumbang kepada atau gagal untuk menghalang kejadian itu.	
5.27 Pembelajaran Daripada Insiden Keselamatan Maklumat (*Learning from Information Security Incidents*)		
ID	**PENERANGAN**	**PERANAN**
5.27.1	**<u>Pembelajaran Daripada Insiden Keselamatan Maklumat (*Learning from Information Security Incidents*)</u>** Pengetahuan yang diperoleh daripada penganalisisan 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 maklumat yang diperoleh daripada penilaian insiden keselamatan maklumat hendaklah digunakan untuk: a) mempertingkatkan pelan pengurusan insiden termasuk senario dan prosedur insiden; b) mengenal pasti insiden berulang atau serius dan puncanya untuk mengemas kini penilaian risiko	ICTSO Pemilik Sistem CSIRT

	keselamatan maklumat organisasi dan menentukan serta melaksanakan kawalan tambahan yang diperlukan untuk mengurangkan kemungkinan atau akibat kejadian serupa pada masa hadapan. Mekanisme untuk membolehkan itu termasuk mengumpul, mengukur dan memantau maklumat tentang jenis insiden, kekerapan insiden dan kos yang terlibat; dan c) meningkatkan kesedaran dan latihan pengguna dengan memberikan contoh tentang perkara yang boleh berlaku, cara bertindak balas terhadap insiden tersebut dan cara mengelak pada masa hadapan.	

5.28 Pengumpulan Bahan Bukti (*Collection of Evidence*)		
ID	**PENERANGAN**	**PERANAN**
5.28.1	**<u>Pengumpulan Bahan Bukti (*Collection of Evidence*)</u>** Kementerian hendaklah menentukan, mewujudkan dan melaksanakan prosedur untuk mengenal pasti dan melindungi maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.	ICTSO Pemilik Sistem CSIRT

5.29 Keselamatan Maklumat Semasa Gangguan (*Information Security During Disruption*)		
ID	**PENERANGAN**	**PERANAN**
5.29.1	**<u>Keselamatan Maklumat Semasa Gangguan (*Information Security During Disruption*)</u>** Keselamatan maklumat semasa gangguan merujuk kepada langkah-langkah dan prosedur yang diambil untuk melindungi dan mengekalkan keselamatan	CDO ICTSO CSIRT Pasukan PKP

	maklumat, data dan sistem komputer semasa terjadi gangguan, bencana, atau insiden yang boleh mengancam integriti dan ketersediaan maklumat. Ini termasuk pelbagai situasi seperti serangan siber, bencana alam, kebakaran, banjir, kecurian atau insiden teknikal yang tidak diingini. Berikut adalah beberapa aspek penting berkaitan dengan keselamatan maklumat semasa gangguan: a) Pembangunan dan pelaksanaan pelan Perancangan Kesinambungan Perkhidmatan (*Business Continuity Planning*) untuk memastikan perniagaan atau operasi organisasi berfungsi dengan minimum gangguan ketika terjadi insiden; b) Pemulihan Bencana (*Disaster Recovery*) melibatkan pelan dan tindakan untuk memulihkan sistem maklumat dan data setelah bencana atau insiden; c) Perlindungan Data (*Protection*) melibatkan salinan data secara berkala, pengekalan data yang baik, dan pelaksanaan tindakan keselamatan yang sesuai untuk melindungi data yang sensitif; d) Pencegahan Serangan Siber (*Cybersecurity Measures*) melibatkan tindakan untuk meminimumkan impak serangan dan melindungi data dari ancaman siber; e) Pemulihan Sistem Cepat (*Quick System Recovery*) untuk mengurangkan masa henti ketika terjadi gangguan; f) Kawalan Fizikal (*Physical Security*) ke bilik server dan peralatan komputer terhad kepada individu yang sah untuk mencegah akses yang tidak diinginkan;	

	g) Pemulihan Data (*Recovery*) memastikan keupayaan untuk memulihkan data yang hilang atau terjejas dalam insiden; h) Keperibadian dan Kesedaran Keselamatan (*Security Awareness*) di dalam organisasi untuk mengurangkan ancaman dalaman dan mencegah insiden yang disebabkan oleh kesalahan manusia; dan i) Pelan Komunikasi Krisis (*Crisis Communication Plan*) yang jelas untuk mengurus krisis dan insiden dengan pantas. Keselamatan maklumat semasa gangguan adalah aspek penting dalam perancangan keselamatan dan keselamatan data, yang memastikan organisasi mampu menjaga integriti, kerahsiaan, dan ketersediaan maklumat penting dalam pelbagai situasi yang mengancam.	

5.30 Kesediaan ICT Bagi Kesinambungan Perkhidmatan (*ICT Readiness for Business Continuity*)		
ID	**PENERANGAN**	**PERANAN**
5.30.1	**<u>Kesinambungan Keselamatan Maklumat (*Information Security Continuity*)</u>** Kesinambungan keselamatan maklumat hendaklah diterapkan dalam pengurusan kesinambungan perkhidmatan Kementerian berdasarkan Pekeliling Am Bilangan 1 Tahun 2025 - Garis Panduan Pengurusan Kesinambungan Perkhidmatan dalam Perkhidmatan Awam *Business Continuity Management* (BCM).	Bahagian Pentadbiran dan Pengurusan Aset ICTSO

5.30.2	**<u>Perancangan Kesinambungan Keselamatan Maklumat (*Planning Information Security Continuity*)</u>** Kementerian hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, Kementerian perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi Kementerian. Kementerian 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: a) Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP) Kementerian; b) Menetapkan polisi PKP; c) Mengenal pasti perkhidmatan kritikal; d) Melaksanakan Kajian Impak Perkhidmatan (*Business Impact Analysis* - BIA) dan Penilaian Risiko terhadap perkhidmatan kritikal; e) Membangunkan Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT; f) Melaksanakan program kesedaran dan latihan pasukan PKP dan Pengguna; g) Melaksanakan simulasi ke atas dokumen; dan h) Melaksanakan penyelenggaraan ke atas pelan.	Jawatankuasa Pemandu PKP Pasukan PKP

5.30.3	**<u>Pelaksanaan Kesinambungan Keselamatan Maklumat (*Implementing Information Security Continuity*)</u>** Kementerian hendaklah menyediakan, mendokumenkan mendokumentasikan, 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: a) Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal Kementerian yang telah dikenal pasti berdasarkan kepada Pelan Kesinambungan Perkhidmatan Kementerian dan DRP; b) Melaksanakan *post-mortem* dan mengemas kini pelan-pelan PKP sekiranya perlu; c) Mengemas kini pelan-pelan PKP jika berlaku perubahan kepada fungsi kritikal Kementerian; d) Mengemas kini struktur tadbir urus PKP Kementerian sekiranya ada perubahan pegawai; dan e) Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP.	Jawatankuasa Pemandu PKP Pasukan PKP
5.30.4	**<u>Menentu sahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat (*Verify, Review and Evaluate Information Security Continuity*)</u>** Kementerian hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan	Jawatankuasa Pemandu PKP Pasukan PKP

	dan dilaksanakan bagi memastikannya sah dan berkesan semasa situasi kecemasan. Kesediaan ICT hendaklah dirancang, dilaksanakan, di selenggara dan diuji berdasarkan objektif kesinambungan perkhidmatan dan keperluan kesinambungan ICT. Organisasi hendaklah memastikan bahawa: a) struktur organisasi yang mencukupi disediakan untuk menyediakan, mengurangkan dan bertindak balas terhadap gangguan yang disokong oleh kakitangan yang mempunyai tanggungjawab, kuasa dan kecekapan yang diperlukan; b) Pelan Kesinambungan Bencana ICT, termasuk tindak balas dan prosedur pemulihan yang memperincikan bagaimana organisasi merancang untuk menguruskan gangguan perkhidmatan ICT; c) Pelan Pemulihan Bencana termasuk maklumat kesinambungan ICT berikut: i. spesifikasi prestasi dan kapasiti untuk memenuhi keperluan dan objektif kesinambungan perkhidmatan seperti yang dinyatakan dalam BIA; ii. Objektif Masa Pemulihan (RTO) bagi setiap perkhidmatan ICT yang diutamakan dan prosedur untuk memulihkan komponen tersebut; dan iii. Objektif Titik Pemulihan (RPO) sumber ICT yang diutamakan ditakrifkan sebagai maklumat dan prosedur untuk memulihkan maklumat.	

5.31 Keperluan Perundangan dan Kontrak (*Legal, Statutory, Regulatory and Contractual Requirements*)		
ID	**PENERANGAN**	**PERANAN**
5.31.1	**Pematuhan Terhadap Keperluan Perundangan dan Kontrak (*Compliance with Legal and Contractual Requirements*)** Meningkat dan memantapkan tahap keselamatan siber bagi mengelak daripada pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.	Warga KKDW Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT KKDW
5.31.2	**Pengenalpastian Keperluan Undang-Undang dan Kontrak yang Terpakai (*Identification of Applicable Legislation and Contractual Agreement*)** Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga Kementerian, pengguna, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian. Keperluan perundangan yang perlu dipatuhi adalah seperti di **LAMPIRAN B** dokumen ini.	Warga KKDW Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT KKDW
5.31.3	**Peraturan Kawalan Kriptografi (*Regulation of Cryptographic Controls*)** Kriptografi ialah bidang yang mempunyai keperluan undang-undang khusus. Penggunaan kriptografi hendaklah mematuhi keperluan perundangan, peraturan, garis panduan dan perjanjian kontrak yang berkaitan antaranya: a) Akta Kerajaan Elektronik 2007; b) Akta Tandatangan Digital 1997;	Warga KKDW Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT KKDW

	c) Dasar Kriptografi Negara; dan d) Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bilangan 3 Tahun 2015 “Dasar Perkhidmatan GPKI”	

5.32 Hak Harta Intelek (*Intellectual Property Rights*)		
ID	**PENERANGAN**	**PERANAN**
5.32.1	**Hak Harta Intelek (*Intellectual Property Rights*)** 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 KKDW Pemilik Sistem Pengurus Projek Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT KKDW

5.33 Perlindungan Rekod (*Protection of Records*)		
ID	**PENERANGAN**	**PERANAN**
5.33.1	**Perlindungan Rekod (*Protection of Records*)** Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, akses tanpa izin dan capaian ke atas orang yang tidak berkenaan.	Warga KKDW Pemilik Sistem Pengurus Projek Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT KKDW

5.34 Privasi dan Perlindungan Peribadi yang boleh dikenal pasti (*Privacy and Protection of Personal Identifiable Information* (PII))		
ID	**PENERANGAN**	**PERANAN**
5.34.1	**<u>Privasi dan Perlindungan Maklumat Peribadi (*Privacy and Protection of Personally Identifiable Information*)</u>** Maklumat peribadi yang boleh dikenal pasti merujuk kepada sebarang data yang boleh digunakan untuk mengenal pasti individu seperti nombor kad pengenalan, rekod perubatan dan lain-lain. Jika terdapat sebarang keperluan terhadap pengenalan tersebut hendaklah terlebih dahulu mendapat persetujuan daripada individu berkenaan. Kementerian hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia. Organisasi hendaklah mengenal pasti dan memenuhi keperluan berkenaan pemeliharaan privasi dan perlindungan maklumat peribadi (PII) mengikut yang berkenaan undang-undang dan peraturan serta keperluan kontrak.	Warga KKDW Pemilik Sistem Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT KKDW
5.35 Kajian Semula Keselamatan Maklumat Secara Berkecuali (*Independent Review of Information Security*)		
ID	**PENERANGAN**	**PERANAN**
5.35.1	**<u>Kajian Semula Keselamatan Maklumat Secara Berkecuali (*Independent Review of Information Security*)</u>** Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang	Pemilik Sistem

	atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	
5.36 Pematuhan Dasar, Peraturan dan Piawaian Untuk Keselamatan Maklumat (*Compliance With Policies, Rules and Standards for Information Security*)		
ID	**PENERANGAN**	**PERANAN**
5.36.1	**<u>Pematuhan ke atas peraturan dan Polisi Standard Keselamatan (*Compliance with Security Policies and Standards*)</u>** Kementerian 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	CDO ICTSO Pemilik Sistem
5.36.2	**<u>Kajian Semula Pematuhan Teknikal (*Technical Compliance Review*)</u>** Kementerian hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung dalam polisi, piawaian dan keperluan komputer.	CDO ICTSO Pemilik Sistem
5.36.3	**<u>Pematuhan peraturan dan dasar kerajaan berkuat kuasa</u>** Memastikan pematuhan ke atas Akta Keselamatan Siber (Akta 854), Peraturan-Peraturan Keselamatan Siber (Tempoh Bagi Penilaian Risiko Keselamatan Siber Dan Audit) 2024 bagi entiti infrastruktur maklumat kritikal negara (NCII) dengan melaksanakan perkara-perkara berikut:	ICTSO

	a) membuat penilaian risiko keselamatan siber sekurang-kurangnya sekali setahun; dan b) menjalankan audit sekurang-kurangnya sekali dalam tiap-tiap dua tahun atau pada kekerapan yang lebih tinggi sebagaimana yang boleh diarahkan oleh Ketua Eksekutif dalam mana-mana hal tertentu.	
5.36.4	**<u>Memastikan semua polisi, peraturan, akta dipatuhi dan di laksana oleh semua peringkat proses perkhidmatan</u>** Semua warga Kementerian , pembekal dan pihak yang terlibat dalam perkhidmatan ICT Kementerian hendaklah mematuhi undang-undang, prosedur, dasar, peraturan yang sedang berkuat kuasa.	ICTSO
5.37 Dokumentasi Prosedur Operasi yang Didokumenkan (*Documented Operating Procedures*)		
ID	**PENERANGAN**	**PERANAN**
5.37.1	**<u>Dokumentasi Prosedur Operasi (*Documented Operating Procedures*)</u>** Semua prosedur operasi hendaklah didokumenkan dan disediakan kepada pihak yang melaksanakan operasi serta mematuhi perkara yang berikut: a) semua prosedur keselamatan siber yang di wujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b) setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan	Pemilik Sistem Pentadbir Sistem

	penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c) semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.	

#6 KAWALAN SUMBER MANUSIA *(PEOPLE CONTROL)*



PKS KKDW V6

6 KAWALAN SUMBER MANUSIA (*PEOPLE CONTROL*)

6.1 Tapisan Keselamatan (*Security Screening*)		
ID	**PENERANGAN**	**PERANAN**
6.1.1	**<u>Tapisan Keselamatan (*Security Screening*)</u>** Tapisan keselamatan hendaklah dijalankan terhadap warga Kementerian, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga Kementerian, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan b) menjalankan tapisan keselamatan untuk warga Kementerian, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Warga KKDW Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT KKDW

6.2 Terma dan Syarat Perkhidmatan (*Terms and Conditions of Employment*)		
ID	**PENERANGAN**	**PERANAN**
6.2.1	**<u>Terma dan Syarat Perkhidmatan (*Terms and Conditions of Employment*)</u>** Persetujuan berkontrak dengan warga Kementerian, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut: a) menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga Kementerian, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian yang terlibat dalam menjamin keselamatan aset ICT; dan b) mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Warga KKDW Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT KKDW
6.3 Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat (*Information Security Awareness, Education and Training*)		
ID	**PENERANGAN**	**PERANAN**
6.3.1	**<u>Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat (*Information Security Awareness, Education and Training*)</u>**	Warga KKDW ICTSO

	Warga Kementerian, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kementerian perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai Polisi Keselamatan Siber KKDW, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) memastikan kesedaran, pendidikan dan latihan diberikan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka; b) memastikan kesedaran yang berkaitan Polisi Keselamatan Siber KKDW perlu diberi dari masa ke semasa; dan c) memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.	Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT KKDW
6.4 Proses Tatatertib (*Disciplinary Process*)		
ID	**PENERANGAN**	**PERANAN**
6.4.1	**<u>Proses Tatatertib (*Disciplinary Process*)</u>** Proses tatatertib yang formal perlu ditentukan dan disampaikan kepada warga Kementerian atau pihak berkepentingan terlibat yang lain bagi membolehkan tindakan diambil ke atas pelanggaran keselamatan	Bahagian Pengurusan Sumber Manusia Unit Integriti

	maklumat yang dilakukan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Memastikan adanya proses tindakan disiplin dan/atau undang-undang sekiranya berlaku pelanggaran terhadap polisi (perundangan dan peraturan yang ditetapkan oleh Kementerian; dan b) Tindakan tatatertib atau digantung daripada mendapat perkhidmatan kepada kemudahan ICT Kementerian akan dikenakan bagi sebarang pelanggaran kepada polisi ini.	

6.5 Tanggungjawab selepas Penamatan atau Pertukaran Pekerjaan (*Responsibilities after Termination or Change of Employment*)		
ID	**PENERANGAN**	**PERANAN**
6.5.1	**<u>Penamatan atau Pertukaran Tanggung Jawab Perkhidmatan (*Termination or Change of Employment Responsibilities*)</u>** Peranan dan tanggungjawab berkaitan keselamatan maklumat yang masih sah selepas penamatan atau pertukaran perjawatan hendaklah ditentukan, dikuatkuasakan dan disampaikan kepada warga Kementerian dan semua pihak yang berkepentingan. Warga Kementerian atau pihak yang berkepentingan terlibat yang lain yang telah tamat perkhidmatan perlu mematuhi perkara-perkara berikut: a) Memastikan semua aset ICT dikembalikan kepada Kementerian mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan	Warga KKDW Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT KKDW Bahagian Pengurusan Maklumat

	kemudahan proses maklumat mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan c) Maklumat rasmi dalam peranti tidak dibenarkan dibawa keluar dari Kementerian. Warga Kementerian yang telah bertukar perkhidmatan hendaklah: a) Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada Kementerian mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan c) Menyedia dan menyerahkan nota serah tugas dan MyPortfolio kepada penyelia yang berkaitan.	

6.6 Perjanjian Kerahsiaan atau Ketakdedahan (*Confidentiality Or Non-Disclosure Agreements*)		
ID	**PENERANGAN**	**PERANAN**
6.6.1	**<u>Perjanjian Kerahsiaan atau Ketakdedahan (*Confidentiality Or Non-Disclosure Agreements*)</u>** Syarat-syarat perjanjian kerahsiaan atau *non-disclosure agreement (NDA)* perlu mengambil kira keperluan organisasi dan hendaklah dikenal pasti, di dokumentasi, disemak secara berkala dan ditandatangani oleh warga Kementerian dan pihak berkepentingan terlibat yang lain.	Warga KKDW Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT KKDW

	Pihak berkepentingan hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.	

6.7 Bekerja Jarak Jauh (*Remote Working*)

ID	PENERANGAN	PERANAN
6.7.1	**<u>Bekerja Jarak Jauh (*Remote Working*)</u>** Dasar dan langkah-langkah keselamatan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan secara jarak jauh. Warga Kementerian yang bekerja secara jarak jauh hendaklah: a) memastikan keselamatan maklumat Kementerian dipatuhi dan tidak disebarkan kepada pihak ketiga; dan b) memastikan arahan bekerja dari luar dipatuhi mengikut garis panduan yang ditetapkan.	Warga KKDW

6.8 Pelaporan Insiden Keselamatan Maklumat (*Reporting Information Security Events*)

ID	PENERANGAN	PERANAN
6.8.1	**<u>Pelaporan Insiden Keselamatan Maklumat (*Reporting Information Security Events*)</u>** Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat berdasarkan pekeliling atau prosedur pengendalian insiden yang sedang berkuat	ICTSO CSIRT

	kuasa. Perkara yang perlu dipatuhi ialah seperti yang berikut: a) Menentukan mekanisme untuk melaporkan sebarang insiden melalui saluran dan dalam tempoh masa yang ditentukan; b) Memberi kesedaran berkaitan prosedur pengendalian insiden dan hebahan kepada warga Kementerian sekiranya terdapat perubahan; dan c) Memastikan warga Kementerian yang mengurus insiden mempunyai kompetensi yang diperlukan. Insiden keselamatan ICT atau ancaman yang berlaku hendaklah dilaporkan kepada CSIRT Kementerian berdasarkan prosedur pengendalian insiden yang sedang berkuat kuasa.	

#7

KAWALAN FIZIKAL *(PHYSICAL CONTROL)*



7 KAWALAN FIZIKAL (*PHYSICAL CONTROL*)

7.1 Perimeter Keselamatan Fizikal (*Physical Security Parameter*)		
ID	**PENERANGAN**	**PERANAN**
7.1.1	**<u>Perimeter Keselamatan Fizikal Perimeter Keselamatan Fizikal (*Physical Security Parameter*)</u>** Kawalan ini bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan Aset ICT Kementerian. Perimeter keselamatan fizikal digunakan untuk melindungi aset, individu, dan persekitaran fizikal daripada ancaman, bahaya, atau kemungkinan kerosakan. Ia melibatkan pelbagai strategi dan tindakan untuk memastikan keselamatan dalam ruang fizikal seperti bangunan, lokasi perindustrian, infrastruktur, atau kawasan penting lain. Berikut adalah beberapa unsur penting yang berkaitan dengan perimeter keselamatan fizikal: a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; b) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; c) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;	Bahagian Pentadbiran dan Pengurusan Aset

	d) Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan manusia; e) Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; f) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan g) Memasang alat penggera atau kamera keselamatan.	
7.2 Kemasukan Fizikal (*Physical Entry*)		
ID	**PENERANGAN**	**PERANAN**
7.2.1	**<u>Kawalan Kemasukan Fizikal (*Physical Entry Controls*)</u>** Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis Kementerian. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Setiap pegawai dan kakitangan Kementerian hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan kepada Kementerian apabila bertukar, tamat perkhidmatan atau bersara; b) Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter	Warga KKDW Pelawat KKDW Pihak yang mempunyai urusan dengan perkhidmatan ICT KKDW

	keselamatan dan hendaklah dikembalikan selepas tamat lawatan; c) Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan Aset ICT Kementerian; d) Kehilangan pas hendaklah dilaporkan segera kepada Pihak Berkuasa; e) Setiap pegawai dan kakitangan Kementerian yang hadir bertugas di luar waktu pejabat hendaklah melaporkan diri ke pos pengawal bagi tujuan rekod kehadiran; dan f) Setiap pelawat hendaklah mendaftar kehadiran di pos pengawal.	
7.2.2	**<u>Kawasan Penyerahan dan Pemunggahan (*Delivery and Loading Areas*)</u>** *Entry point* seperti kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan. Pihak Kementerian hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.	Bahagian Pentadbiran dan Pengurusan Aset

7.3 Keselamatan Pejabat, Bilik dan Kemudahan (*Securing Offices, Rooms and Facilities*)		
ID	**PENERANGAN**	**PERANAN**
7.3.1	**<u>Keselamatan Pejabat, Bilik dan Kemudahan (*Securing Office, Rooms and Facilities*)</u>** 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 krisis, 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 KKDW Bahagian Pentadbiran dan Pengurusan Aset Pentadbir Pusat Data

7.4 Pemantauan Keselamatan Fizikal (*Physical Security Monitoring*)		
ID	**PENERANGAN**	**PERANAN**
7.4.1	**<u>Pemantauan Keselamatan Fizikal (*Physical Security Monitoring*)</u>** Premis fizikal harus dipantau oleh sistem pengawasan termasuk pengawal, penggera penceroboh, sistem pemantauan video seperti kamera litar tertutup (CCTV) dan perisian pengurusan maklumat keselamatan fizikal sama ada diurus secara dalaman atau oleh penyedia perkhidmatan pemantauan.	Bahagian Pentadbiran dan Pengurusan Aset Pentadbir Pusat Data

	Sistem pemantauan harus dilindungi daripada capaian yang tidak dibenarkan untuk mengelakkan maklumat pengawasan, seperti suapan video, daripada diakses oleh orang yang tidak dibenarkan atau sistem dicerobohi secara jarak jauh. Melaksanakan pemantauan secara berterusan di premis bagi mengelakkan akses fizikal yang tidak dibenarkan. Akses kepada bangunan yang menempatkan sistem kritikal harus dipantau secara berterusan untuk mengesan akses yang tidak dibenarkan atau tingkah laku yang mencurigakan dengan: a) memasang sistem pemantauan video seperti kamera litar tertutup (CCTV) untuk melihat dan merakam akses ke kawasan sensitif di dalam dan di luar premis organisasi; dan b) perlindungan juga perlu disediakan untuk kawasan lain (contoh: komputer atau bilik komunikasi).	
7.5 Perlindungan Daripada Ancaman Fizikal Dan Persekitaran *(Protecting Against Physical and Environmental Threats*)		
ID	**PENERANGAN**	**PERANAN**
7.5.1	**<u>Perlindungan Daripada Ancaman Fizikal Dan Persekitaran (*Protecting Against Physical and Environmental Threats*)</u>** Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. Kementerian perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.	Pentadbir Pusat Data Bahagian Pentadbiran dan Pengurusan Aset

7.6 Bekerja di Kawasan Selamat (*Working In Secure Areas*)		
ID	**PENERANGAN**	**PERANAN**
7.6.1	**<u>Bekerja di Kawasan Selamat (*Working in Secure Area*)</u>** Langkah-langkah kawalan keselamatan bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada warga Kementerian yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis Kementerian termasuklah Pusat Data. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Langkah-langkah kawalan keselamatan ke atas kawasan tersebut ialah seperti yang berikut: a) 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; b) Akses adalah terhad kepada warga Kementerian yang telah diberi kuasa sahaja dan dipantau pada setiap masa; c) Pemantauan dibuat menggunakan CCTV atau lain-lain peralatan yang sesuai; d) Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual;	Pentadbir Pusat Data Bahagian Pentadbiran dan Pengurusan Aset

	e) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; f) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; g) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam; h) Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan; i) Memperkukuh dinding dan siling; dan j) Mengehadkan jalan keluar masuk.	
7.7 Meja Kosong dan Skrin Kosong (*Clear Desk and Clear Screen*)		
ID	**PENERANGAN**	**PERANAN**
7.7.1	**<u>Polisi Meja Kosong dan Skrin Kosong (*Clear Desk Clear Screen Policy*)</u>** *Clear Desk* bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada atas meja pengguna atau di skrin komputer apabila pengguna tidak berada di tempatnya. "Polisi Meja Kosong dan Skrin Kosong" adalah satu set garis panduan yang digunakan dalam pengurusan keselamatan maklumat dan keberkesanan dalam organisasi untuk melindungi maklumat sensitif dan menjaga privasi pekerja. Objektif utama polisi ini adalah untuk memastikan meja kerja dan skrin komputer teratur dan selamat bagi	Warga KKDW

	mengelakkan kecurian atau kehilangan maklumat. Ini merangkumi aspek-aspek berikut: a) Penggunaan fungsi *password screensaver* atau *logout* apabila meninggalkan komputer; b) Pengaktifan fungsi "*Sleep Mode*"; c) Penyimpanan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; d) Semua dokumen hendaklah diambil segera daripada pencetak, pengimbas, mesin faksimile dan mesin fotokopi; e) Pengawalan E-mel masuk dan keluar; f) Kawalan penggunaan mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital; g) Penetapan dan hebahan peraturan serta panduan berkaitan konfigurasi *pop-up* di skrin (cth. mematikan *pop-up* e-mel dan mesej baharu semasa pembentangan, perkongsian skrin atau di kawasan awam); dan h) membersihkan maklumat sensitif atau kritikal pada papan putih dan jenis paparan lain apabila tidak diperlukan lagi.	
7.7.2	**<u>Peralatan Pengguna Tanpa Kawalan (*Unattended User Equipment*)</u>** 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: a) Tamatkan sesi aktif apabila selesai tugas;	Warga KKDW

	b) *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan c) Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.	

7.8 Penempatan dan Perlindungan Peralatan ICT (*Equipment Siting and Protection*)		
ID	**PENERANGAN**	**PERANAN**
7.8.1	**<u>Penempatan dan Perlindungan Peralatan ICT (*Equipment Siting and Protection*)</u>** Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut: a) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem; e) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif	Warga KKDW Pegawai Aset

	(*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; f) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna; g) Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; h) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set* (Gen-Set); i) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; j) Peralatan rangkaian seperti suis, penghala, hab dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci; k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; l) Peralatan ICT yang hendak dibawa ke luar premis Kementerian, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan; m) Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden; n) Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;	

	o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pegawai Aset; p) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pegawai Aset untuk dibaik pulih; q) Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; r) Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal; s) Pengguna dilarang sama sekali mengubah *password administrator* yang telah ditetapkan oleh pihak ICT; dan t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi kerajaan dan Kementerian sahaja.	

7.9 Keselamatan Aset di Luar Premis (*Security of Assets Off-Premises*)		
ID	**PENERANGAN**	**PERANAN**
7.9.1	**<u>Keselamatan Aset di Luar Premis (*Security of Equipment Off-Premises*)</u>** Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis Kementerian. Peralatan yang dibawa keluar dari premis Kementerian adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti yang berikut:	Warga KKDW Pembekal Pihak yang mempunyai urusan berkaitan perkhidmatan ICT KKDW

	a) Peralatan perlu dilindungi dan dikawal sepanjang masa; b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan c) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.	

7.10 Media Storan (*Storage Media*)		
ID	**PENERANGAN**	**PERANAN**
7.10.1	**<u>Pengurusan Media Boleh Alih (*Management of Removal Media*)</u>** Untuk mengelakkan kerosakan pada aset dan gangguan kepada aktiviti perkhidmatan, media harus dikawal dan dilindungi secara fizikal. Pemacu media boleh alih harus dibolehkan jika terdapat keperluan untuk berbuat demikian. Media boleh alih mesti dikendalikan mengikut klasifikasi maklumat. 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	Warga KKDW Pegawai Aset

	kerosakan dan pendedahan yang tidak dibenarkan; dan e) Menyimpan semua jenis media di tempat yang selamat.	
7.10.2	**<u>Pelupusan Media (*Disposal of Media*)</u>** a) Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan; dan b) Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	Pegawai Aset Jawatankuasa yang dilantik untuk pelupusan aset
7.10.3	**<u>Pengalihan Aset (*Removal of Assets*)</u>** Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: a) Peralatan ICT yang hendak dibawa keluar dari premis Kementerian untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Setiausaha atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan b) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.	Warga KKDW Pegawai Aset

7.10.4	**<u>Pengendalian Media (*Media Handling*)</u>** Melindungi aset maklumat daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	Warga KKDW Pentadbir Sistem

7.11 Utiliti Sokongan (*Supporting Utilities*)		
ID	**PENERANGAN**	**PERANAN**
7.11.1	**<u>Utiliti Sokongan (*Supporting Utilities*)</u>** Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Semua alat sokongan perlu di selenggara dari semasa ke semasa (sekurang-kurangnya setahun sekali).	Pegawai Aset Bahagian Pentadbiran dan Pengurusan Aset

7.12 Keselamatan Kabel (*Cabling Security*)		
ID	**PENERANGAN**	**PERANAN**
7.12.1	**<u>Keselamatan Kabel (*Cabling Security*)</u>** 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.	Pentadbir Sistem

	Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut: a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	

7.13 Penyelenggaraan Peralatan (*Equipment Maintenance*)		
ID	**PENERANGAN**	**PERANAN**
7.13.1	**<u>Penyelenggaraan Peralatan (*Equipment Maintenance*)</u>** Peralatan ICT hendaklah di selenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. Perkakasan hendaklah di selenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: a) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; b) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang di selenggara;	Pegawai Aset Pentadbir Sistem

	c) Memastikan perkakasan hanya di selenggara oleh kakitangan atau pihak yang dibenarkan sahaja; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	

7.14 Pelupusan yang Selamat atau Penggunaan Semula Peralatan (*Secure Disposal or Re-Use of Equipment*)		
ID	**PENERANGAN**	**PERANAN**
7.14.1	**<u>Pelupusan yang Selamat atau Penggunaan Semula Peralatan (*Secure Disposal or Re-Use of Equipment*)</u>** Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (*overwrite*) sebelum dilupuskan atau diguna semula. Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki yang dibekalkan oleh Kementerian dan ditempatkan di Kementerian. Peralatan ICT yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuat kuasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan Kementerian. Langkah-langkah seperti yang berikut hendaklah diambil: a) Bagi peralatan ICT yang akan dilupuskan sebelum di pindah milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat;	Pegawai Aset Pentadbir Sistem Warga KKDW

	b) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; c) Peralatan yang hendak di lupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; d) Pelupusan peralatan ICT hendaklah dilakukan mengikut tatacara pelupusan semasa yang berkuat kuasa; e) Warga Kementerian adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti yang berikut: i) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi; ii) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *Hard Disk*, *Motherboard* dan sebagainya; iii) Menyimpan dan memindahkan perkakasan luaran komputer seperti *Uninterrupted Power Supply* (UPS), pembesar suara atau mana-mana peralatan yang berkaitan ke mana-mana bahagian di Kementerian; iv) Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; dan v) Melupuskan sendiri peralatan ICT. f) Warga Kementerian bertanggungjawab memastikan segala maklumat rasmi di dalam aset ICT disalin pada media storan kedua atau mana-mana media storan mudah alih sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan atau dipindah milik bagi tujuan sandaran maklumat.	

	g) Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang berkuat kuasa; h) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan i) Pegawai aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT.	

#8

KAWALAN TEKNOLOGI *(TECHNOLOGICAL CONTROL)*



PKS KKDW V6

8 KAWALAN TEKNOLOGI (*TECHNOLOGICAL CONTROL*)

8.1 Peranti Titik Hujung Pengguna (*User Endpoint Devices*)		
ID	**PENERANGAN**	**PERANAN**
8.1.1	**<u>Polisi Peranti Mudah Alih (*Mobile Device Policy*)</u>** Polisi dan langkah-langkah keselamatan sokongan hendaklah digunakan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih. Kementerian perlu membangun serta menyebarkan dasar dan langkah-langkah keselamatan sokongan bagi mengurus risiko yang dikenal pasti melalui penggunaan peranti akhir (*endpoint device*) merangkumi antara perkara berikut: a) jenis maklumat dan tahap klasifikasi yang digunakan oleh pengguna peranti akhir untuk mengendali, memproses, menyimpan atau menyokong kemudahan maklumat; b) peraturan untuk capaian kepada perkhidmatan maklumat, rangkaian awam atau mana-mana rangkaian lain di luar premis; c) penyulitan peranti storan; d) perlindungan terhadap virus dan perisian hasad (*malware*); e) Menyekat keupayaan jarak jauh (*remote disabling*), pemadaman dan penguncian (*lockout*); f) sandaran (*back up*); g) penggunaan perkhidmatan web dan aplikasi web; h) analisis tingkah laku pengguna akhir; i) penggunaan perkhidmatan boleh alih, termasuk peranti memori boleh alih, dan kemungkinan	ICTSO Warga KKDW

	membatalkan keupayaan *port* fizikal (contoh: *port USB*, *USB Type-C*); dan i) penggunaan keupayaan pembahagian, (*partitioning capabilities*), jika disokong oleh peranti akhir pengguna.	
8.2 Hak Akses Istimewa (*Privileged Access Rights*)		
ID	**PENERANGAN**	**PERANAN**
8.2.1	**<u>Pengurusan Hak Akses Istimewa (*Management of Privileged Access Rights*)</u>** Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak akses perlu diberikan kawalan dan penyeliaan yang ketat mengikut keperluan skop tugas yang telah dikenal pasti berdasarkan prosedur yang berkuat kuasa.	Pentadbir Sistem
8.3 Sekatan Akses Maklumat (*Information Access Restriction*)		
ID	**PENERANGAN**	**PERANAN**
8.3.1	**<u>Sekatan Akses Maklumat (*Information Access Restriction*)</u>** Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian merangkumi perkara berikut: a) tidak membenarkan pengguna yang tidak berdaftar mencapai maklumat sensitif; b) menyediakan mekanisme konfigurasi untuk mengawal capaian kepada maklumat dalam sistem, aplikasi dan perkhidmatan;	Pentadbir Sistem Pemilik Sistem

	c) mengawal data yang boleh diakses oleh pengguna tertentu; d) mengawal identiti atau kumpulan identiti yang mempunyai akses, seperti membaca, menulis, memadam dan melaksanakan (*execute*); e) menyediakan kawalan capaian fizikal atau logikal untuk mengasingkan aplikasi sensitif, data aplikasi, atau sistem; dan f) Melaksanakan semakan dan pemantauan **sekali dalam tempoh setahun (1) atau bila perlu** bagi memastikan pengguna yang mencapai sistem adalah sah. Penggunaan proses dan teknik pengurusan capaian yang dinamik (*dynamic access management*) bagi melindungi maklumat sensitif perlu dilaksanakan sekiranya diperlukan dengan mengambil kira keperluan berikut: a) perlindungan sepanjang kitar hayat maklumat dengan menetapkan peraturan berdasarkan kes penggunaan; b) mewujudkan operasi, proses memantau dan melapor serta infrastruktur sokongan teknikal; dan c) melindungi data dengan menetapkan keperluan pengesahan, mengehadkan capaian, melaksanakan penyulitan, menetapkan kebenaran mencetak, merekod capaian pengguna dan penggunaan maklumat serta memberikan amaran sekiranya terdapat percubaan untuk menyalahgunakan maklumat.	

8.4 Kawalan Akses kepada Kod Sumber Program (*Access Control to Source Code*)		
ID	**PENERANGAN**	**PERANAN**
8.4.1	**<u>Kawalan Akses Kepada Kod Sumber Program (*Access Control to Source Code*)</u>** Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu boleh dipertimbangkan adalah seperti yang berikut: a) Log audit perlu dikekalkan kepada semua akses kepada kod sumber; b) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; c) Kod sumber bagi semua aplikasi dan perisian yang dibangunkan hendaklah menjadi hak milik Kementerian. d) Menguruskan capaian kepada kod sumber program dan perpustakaan sumber program (*program source libraries*) mengikut prosedur yang ditetapkan; dan e) Memberi akses baca dan tulis kepada kod sumber berdasarkan keperluan dan berupaya mengawal risiko mengubah atau menyalah guna kod sumber mengikut prosedur yang ditetapkan.	Pengurus Projek Pentadbir Sistem Pembekal
8.5 Pengesahan Selamat (*Secure Authentication*)		
ID	**PENERANGAN**	**PERANAN**
8.5.1	**<u>Prosedur Log Masuk yang Selamat (*Secure Log-On Procedure*)</u>** Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah	Pentadbir Sistem Pemilik Sistem

	kawalan yang boleh digunakan adalah seperti yang berikut: a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Kementerian**;** b) Menjana amaran (*alert*) sekiranya berlaku perlanggaran semasa proses log maşuk terhadap aplikasi sistem; c) Mengawal capaian ke atas aplikasi sistem mengikut prosedur yang ditetapkan ; d) Mewujudkan teknik pengesahan pelbagai faktor (*multi factor authentication* - MFA) berdasarkan klasifikasi maklumat yang bersesuaian bagi mengesahkan pengenalan diri pengguna; e) Mewujudkan sistem pengurusan kata laluan dan memastikan kata laluan yang kukuh dan berkualiti; dan f) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	
8.5.2	**<u>Sistem Pengurusan Kata Laluan (*Password Management System*)</u>** Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh kementerian seperti yang berikut: a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau di kompromi; c) Panjang kata laluan mestilah sekurang- kurangnya **DUA BELAS (12) AKSARA** dengan gabungan	Pentadbir Sistem Pemilik Sistem Warga KKDW

	antara huruf, aksara khas dan nombor (*alphanumeric*) **KECUALI** bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad; d) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekali pun; e) Kata laluan paparan kunci (*lock screen*) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara; g) Kuat kuasakan pertukaran kata laluan semasa atau selepas login kali pertama atau selepas reset kata laluan; h) kata laluan tidak berdasarkan perkataan kamus atau gabungannya; i) kata laluan yang sama tidak digunakan merentas perkhidmatan dan sistem yang berbeza; j) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; k) Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum **TIGA (3) KALI** sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga ID capaian diaktifkan semula; dan l) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	

8.6 Pengurusan Kapasiti (*Capacity Management*)		
ID	**PENERANGAN**	**PERANAN**
8.6.1	**<u>Pengurusan Kapasiti (*Capacity Management*)</u>** 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 dipertimbangkan adalah seperti yang berikut: 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; b) kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang; dan c) Mempertimbangkan penggunaan pengkomputeran awan bagi pengurusan kapasiti yang berkesan, anjal (*elasticity*) dan boleh skala (*scalability*).	Pemilik Sistem Pentadbir Sistem
8.7 Perlindungan daripada Perisian Hasad (*Protection Against Malware*)		
ID	**PENERANGAN**	**PERANAN**
8.7.1	**<u>Perlindungan daripada Perisian Hasad (*Protection Against Malware*)</u>** Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada serangan *malware*	Pentadbir Sistem Pengguna

	hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. Perkara yang perlu dilaksanakan bagi memastikan perlindungan aset maklumat daripada perisian berbahaya ialah seperti yang berikut: a) Memasang sistem keselamatan untuk mengesan perisian atau program *malware* seperti antivirus, *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS) dan *Web Application Firewall* (WAF) serta mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c) Mengimbas semua perisian atau sistem dengan antivirus mengikut keperluan~~;~~ d) Mengemas kini antivirus dengan *signature/pattern* antivirus yang terkini; e) Menyemak kandungan sistem atau maklumat sekali dalam setahun atau sekiranya perlu bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;	

	h) menyediakan pelan kesinambungan perkhidmatan yang sesuai untuk pulih daripada serangan perisian hasad; i) menentukan prosedur dan tanggungjawab untuk menangani perlindungan terhadap perisian hasad pada sistem; dan j) mengesahkan ketepatan sumber maklumat yang berkaitan dengan perisian hasad.	
8.8 Pengurusan Kerentanan Teknikal (*Management of Technical Vulnerabilities*)		
ID	**PENERANGAN**	**PERANAN**
8.8.1	**<u>Pengurusan Kerentanan Teknikal (*Management of Technical Vulnerabilities*)</u>** Maklumat berkaitan kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. Kawalan terhadap keterdedahan teknikal perlu dilaksanakan untuk melindungi sistem maklumat, perisian, dan infrastruktur teknikal organisasi daripada ancaman dan serangan yang berkaitan dengan kerentanan. Perkara yang perlu dipatuhi ialah seperti yang berikut: a) Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi; b) Mengenal pasti, menilai dan menganalisis tahap risiko kerentanan yang wujud dalam sistem, perisian, dan rangkaian Kementerian;	Pentadbir Sistem Pemilik Sistem

	c) Melaksanakan tindakan penambahbaikan untuk mengatasi kerentanan yang telah dikenal pasti, termasuk melaksanakan penambahbaikan keselamatan dan konfigurasi semula; d) Memantau sistem dan perisian secara berterusan untuk mengenal pasti kerentanan yang mungkin muncul dalam masa sebenar; dan e) Melaksana dan memastikan amalan terbaik dalam keselamatan teknikal dan pengurusan kerentanan.	
8.9 Pengurusan konfigurasi (*Configuration Management*)		
ID	**PENERANGAN**	**PERANAN**
8.9.1	**<u>Pengurusan Konfigurasi (*Configuration Management*)</u>** Pengurusan konfigurasi perlu dilaksanakan untuk memastikan perkakasan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul berserta dengan keperluan keselamatan dan konfigurasi tidak diubah tanpa kebenaran berdasarkan prosedur yang ditetapkan. Perkara yang perlu dipatuhi ialah seperti yang berikut: a) Melindungi capaian terhadap fail konfigurasi mengikut kawalan yang ditetapkan; b) Merekod dan menyimpan sebarang perubahan konfigurasi dengan selamat; dan c) Memantau konfigurasi untuk mengesahkan tetapan konfigurasi dan menilai kawalan keselamatan.	Pentadbir Sistem

8.10 Penghapusan Maklumat (*Information Deletion*)		
ID	**PENERANGAN**	**PERANAN**
8.10.1	**<u>Penghapusan Maklumat (*Information Deletion*)</u>** Data terperingkat dalam sistem maklumat, peralatan atau media storan yang lain hendaklah dilupuskan mengikut prosedur yang ditetapkan. Perkara yang perlu dipatuhi ialah seperti berikut: a) Menentukan kaedah penghapusan maklumat yang sesuai selaras dengan keperluan Kementerian; b) Merekod keputusan sebagai bukti penghapusan maklumat; dan c) Mendapatkan bukti penghapusan maklumat jika menggunakan perkhidmatan pembekal.	Pemilik Sistem Pengguna Aset Pegawai Aset
8.11 Penyamaran Data (*Data Masking*)		
ID	**PENERANGAN**	**PERANAN**
8.11.1	**<u>Penyamaran Data (*Masking*)</u>** Penyamaran data (*masking*) dilaksana bagi melindungi data sensitif seperti data *Personal Identifiable Information* (PII) dan data terperingkat dengan mengambil kira keperluan perkhidmatan dan polisi kawalan capaian serta polisi lain yang berkaitan tertakluk kepada keperluan perundangan dan peraturan yang berkuat kuasa. Pelaksanaan penyamaran data ialah berdasarkan prosedur yang ditetapkan. Penyamaran data diperlukan bagi melindungi data PII dan data sensitif daripada terdedah atau bocor kepada pihak yang tidak bertanggung jawab yang akan menyebabkan	Pentadbir Sistem Pemilik Sistem

	imej Kementerian terjejas. Perkara yang perlu dipatuhi ialah seperti yang berikut: a) Mengenal pasti klasifikasi data yang perlu dikongsi dengan pihak ketiga; b) Mengenal pasti teknik yang sesuai selaras dengan sensitiviti data; dan c) Memastikan pengguna hanya dapat mencapai data yang minimum yang dibenarkan sahaja.	

8.12 Pencegahan Ketirisan Data (*Data Leakage Prevention*)

ID	PENERANGAN	PERANAN
8.12.1	**<u>Pencegahan Ketirisan Data (*Data Leakage Prevention*)</u>** Data dalam sistem, rangkaian dan peralatan lain perlu dilindungi daripada pendedahan dan pengekstrakan data yang tidak sah oleh individu atau sistem. Perkara yang perlu dipatuhi ialah seperti berikut: a) mengenal pasti dan mengelas maklumat untuk dilindungi daripada ketirisan; b) memantau saluran transaksi dan perkongsian data (contoh: e-mel, pemindahan fail, *mobile services*, media boleh alih); dan c) laksanakan tindakan pengukuhan untuk mengelakkan ketirisan maklumat.	Pentadbir Sistem Pemilik Sistem

8.13 Sandaran Maklumat (*Information Backup*)		
ID	**PENERANGAN**	**PERANAN**
8.13.1	**<u>Sandaran Maklumat (*Information Backup*)</u>** Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara berkala mengikut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di *off-site*. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: a) Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b) Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi; c) Menguji sistem sandaran sedia ada secara berkala bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana; dan d) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara **harian, mingguan, bulanan atau tahunan**. Kekerapan sandaran bergantung pada tahap kritikal maklumat, dan hendaklah disimpan sekurang-kurangnya **TIGA (3) GENERASI**.	Pentadbir Sistem

8.14 Lewahan bagi Kemudahan Pemprosesan Maklumat (*Redundancy of Information Processing Facilities*)		
ID	**PENERANGAN**	**PERANAN**
8.14.1	**<u>Lewahan bagi Kemudahan Pemprosesan Maklumat (*Redundancy of Information Processing Facilities*)</u>** Kementerian perlu mengenal pasti keperluan, mereka bentuk dan melaksanakan lewahan untuk memastikan kesinambungan perkhidmatan dan ketersediaan kemudahan pemprosesan maklumat. Perkara yang perlu dipatuhi ialah seperti yang berikut: a) Mengenal pasti keperluan dan tahap kritikal bagi ketersediaan perkhidmatan dan sistem maklumat; b) Menyediakan lewahan bagi kemudahan pemprosesan maklumat yang dikenal pasti; c) Menguji keberkesanan (*failover testing*) untuk memastikan keberkesanan kemudahan lewahan secara berkala; dan d) Menyediakan mekanisme yang bersesuaian untuk memberi amaran gangguan atau kegagalan kemudahan pemprosesan maklumat kepada Kementerian untuk memastikan lewahan tersebut boleh mengambil alih fungsi kemudahan utama dibaiki atau diganti.	Pentadbir Pusat Data Pemilik Sistem Pentadbir Sistem
8.15 Menyediakan Log (*Logging*)		
ID	**PENERANGAN**	**PERANAN**
8.15.1	**<u>Menyediakan Log (*Logging*)</u>** Kementerian perlu merekod aktiviti dan menjana bahan bukti untuk memastikan maklumat log adalah berintegriti dan boleh digunakan sebagai bahan bukti jika berlaku	Pentadbir Sistem

	insiden keselamatan maklumat. Perkara yang perlu dipatuhi ialah seperti yang berikut: a) menyedia, menyimpan, melindungi dan menganalisis log yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa berkaitan keselamatan maklumat. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem; b) Log hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan; c) 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 yang berikut: i. Fail log sistem pengoperasian; ii. Fail log servis (contoh: web, e-mel); iii. Fail log aplikasi (*audit trail*); dan iv. Fail log rangkaian (contoh: *switch*, *firewall*, IPS).	
8.15.2	**<u>Perlindungan Maklumat Log (*Protection of Log Information*)</u>** Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada perubahan dan capaian tanpa izin merangkumi perkara berikut:	Pentadbir Sistem

	a. Pengguna, termasuk mereka yang mempunyai hak akses istimewa, tidak diberi kebenaran untuk memadam atau menyahaktifkan log aktiviti mereka sendiri; dan b. Kemudahan pengelogan beroperasi dengan baik.	
8.15.3	**<u>Analisis log (*Log Analysis*)</u>** Analisis log perlu merangkumi analisis dan interpretasi aktiviti keselamatan maklumat untuk mengenal pasti aktiviti yang luar biasa atau tingkah laku yang janggal yang menunjukkan indikator sistem terjejas. Perkara yang perlu dipatuhi ialah seperti yang berikut: a) Memantau penggunaan kemudahan memproses maklumat secara berkala; b) Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak secara berkala dan laporan perlu disediakan jika perlu; c) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; d) Log Audit yang merekodkan semua aktiviti perlu diwujudkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan e) Aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkannya kepada pasukan CSIRT Kementerian.	Pentadbir Sistem

8.16 Aktiviti Pemantauan (*Monitoring Activities*)		
ID	**PENERANGAN**	**PERANAN**
8.16.1	**<u>Aktiviti Pemantauan (*Monitoring Activities*)</u>** Rangkaian, sistem dan aplikasi harus dipantau dan tindakan sewajarnya diambil untuk menilai kemungkinan insiden keselamatan maklumat. Kementerian perlu memantau untuk mengesan tingkah laku tidak normal (anomali) dan kemungkinan berlaku insiden keselamatan maklumat. Aktiviti pemantauan perlu merangkumi perkara seperti berikut: a) trafik keluar (*outbound*) dan masuk (*inbound*) bagi rangkaian, sistem dan aplikasi; b) capaian kepada sistem, pelayan, peralatan rangkaian, sistem pemantauan, aplikasi kritikal; c) log daripada peralatan keselamatan [contoh: antivirus, IDS, sistem pencegahan pencerobohan (IPS), penapis web, *firewall*, pencegahan kebocoran data]; d) log peristiwa yang berkaitan dengan sistem dan aktiviti rangkaian; e) memastikan supaya kod yang dilaksanakan telah diberi kebenaran untuk dilaksanakan dan ia tidak diubah tanpa kebenaran ; dan f) penggunaan dan prestasi sumber.	Pentadbir Sistem CSIRT

8.17 Penyeragaman Jam (*Clock Synchronization*)		
ID	**PENERANGAN**	**PERANAN**
8.17.1	**<u>Penyeragaman Jam (*Clock Synchronisation*)</u>** Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut waktu piawai Malaysia. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam Kementerian atau domain keselamatan perlu diseragamkan dengan waktu piawai Malaysia yang ditetapkan oleh *National Metrology Institute of Malaysia* (NMIM).	Pentadbir Pusat Data
8.18 Penggunaan Program Utiliti yang Mempunyai Hak Istimewa (*Use of Privileged Utility Programs*)		
ID	**PENERANGAN**	**PERANAN**
8.18.1	**<u>Penggunaan Program Utiliti yang Mempunyai Hak Istimewa (*Use of Privileged Utility Programs*)</u>** Penggunaan program utiliti yang mungkin boleh *overriding system* perlu dihadkan hanya kepada Pentadbir Sistem dan dikawal ketat penggunaannya. Perkara yang perlu dipatuhi ialah seperti yang berikut: a) had penggunaan program utiliti kepada bilangan praktikal minimum pengguna yang dipercayai dan dibenarkan; b) kebenaran untuk menggunakan program utiliti secara *ad hoc*;	Pentadbir Sistem

	c) Melaksanakan pengasingan tugas dengan mengehadkan capaian pengguna yang mempunyai akses kepada program utiliti; d) Membuat *housekeeping* program utiliti yang tidak diperlukan; dan e) pengelogan penggunaan program utiliti penting.	
8.19 Pemasangan Perisian pada Sistem yang Beroperasi (*Installation of Software on Operational Systems*)		
ID	**PENERANGAN**	**PERANAN**
8.19.1	**<u>Pemasangan Perisian pada Sistem yang Beroperasi (*Installation of Software on Operational Systems*)</u>** Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada mana-mana sistem yang beroperasi berdasarkan langkah-langkah berikut: a) Strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian; b) Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperakui berjaya; c) Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur; d) Pengemaskinian perisian operasi hanya boleh dilaksanakan oleh pentadbir terlatih atas kebenaran pengurusan; e) Memastikan bahawa hanya kod boleh laksana (*executable code*) yang telah diluluskan dan tiada kod pembangunan atau penyusun (*compilers*) dipasang pada sistem operasi; f) Mengemas kini semua perpustakaan sumber (*source libraries*) program yang sepadan;	Pentadbir Sistem

	g) Pengurusan rekod konfigurasi hendaklah dilaksanakan secara teratur, disemak secara berkala dan disimpan dengan selamat; dan h) Versi lama perisian perlu diarkib bersama dengan maklumat dan parameter, prosedur, maklumat konfigurasi terperinci dan perisian yang menyokongnya selama mana data boleh disimpan di dalam arkib (*archive*) bagi sistem tertentu.	
8.19.2	**<u>Sekatan ke atas Pemasangan Perisian (*Restriction on Software Installation*)</u>** Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) hanya perisian yang rasmi sahaja dibenarkan bagi kegunaan jabatan; b) lesen perisian (*registration code, serials, product key*) perlu disimpan berasingan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; c) kod sumber (*source code*) sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan; d) sistem aplikasi, perisian dan kod sumber tidak dibenarkan dikongsi, diagih, dibawa keluar atau didemontrasikan kepada pihak lain kecuali dengan kebenaran Pengurus ICT; dan e) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang- undang bertulis yang berkuat kuasa.	Warga KKDW Pentadbir Sistem

8.20 Keselamatan Rangkaian (*Networks Security*)		
ID	**PENERANGAN**	**PERANAN**
8.20.1	**<u>Kawalan Rangkaian (*Network Control*)</u>** Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara yang perlu dipatuhi adalah seperti berikut : a) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; b) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas daripada risiko seperti banjir, gegaran dan habuk; c) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja; d) Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e) *Firewall* hendaklah dipasang, di konfigurasi dan diselia oleh Pentadbir Rangkaian; f) Semua trafik keluar dan masuk rangkaian hendaklah melalui firewall di bawah kawalan Kementerian; g) Semua perisian *sniffer* atau *network analyse*r adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran daripada ICTSO; h) Memasang perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan	Pentadbir Rangkaian

	pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat Kementerian; i) Memasang *Web Content Filtering* pada Internet *Gateway* bagi menyekat aktiviti yang dilarang; j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan Kementerian adalah tidak dibenarkan; k) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di jabatan sahaja dan penggunaan modem persendirian adalah dilarang sama sekali; l) Kemudahan bagi *wireless* LAN hendaklah dipantau dan dikawal penggunaannya; m) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja; n) Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh; dan o) Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) bagi memastikan pematuhan terhadap peraturan di Kementerian.	
8.21 Keselamatan Perkhidmatan Rangkaian (*Security of Network Services*)		
ID	**PENERANGAN**	**PERANAN**
8.21.1	**<u>Keselamatan Perkhidmatan Rangkaian (*Security of Network Services*)</u>** Pengurusan bagi semua perkhidmatan rangkaian (*inhouse* atau *outsource*) yang merangkumi mekanisme keselamatan dan tahap serta keperluan perkhidmatan	ICTSO Pentadbir Rangkaian

	rangkaian hendaklah dikenal pasti dan dimasukkan dalam perjanjian perkhidmatan.	
8.22 Pengasingan dalam Rangkaian (*Segregation of Networks*)		
ID	**PENERANGAN**	**PERANAN**
8.22.1	**<u>Pengasingan dalam Rangkaian (*Segregation in Networks*)</u>** Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian Kementerian.	Pentadbir Rangkaian
8.23 Penyaringan Web (*Web Filtering*)		
ID	**PENERANGAN**	**PERANAN**
8.23.1	**<u>Penyaringan Web (*Web Filtering*)</u>** Kawalan penyaringan web dalam bentuk perisian atau sebagainya perlu dilaksanakan bagi mengesan dan menyekat ke laman web yang dianggap tidak selamat dan tidak sesuai. Ini bagi melindungi sistem maklumat daripada sebarang ancaman keselamatan laman web luaran. Risiko mengakses laman web yang mengandungi maklumat yang dilarang atau diketahui mengandungi virus atau bahan pancingan (*phishing*) data oleh pengguna perlu dikurangkan. Langkah yang perlu diambil untuk menyekat akses adalah seperti berikut:	Pentadbir Rangkaian

	a) Laman web yang diketahui atau disyaki mengandungi bahan berniat jahat, seperti laman web dengan kandungan perisian yang tidak selamat; b) Laman web berniat jahat yang diperoleh daripada *scammer*; dan c) Laman web yang mengedarkan kandungan dan bahan yang menyalahi undang-undang.	
8.24 Penggunaan Kriptografi (*Use of Cryptography*)		
ID	**PENERANGAN**	**PERANAN**
8.24.1	**<u>Polisi Penggunaan Kawalan Kriptografi (*Policy on The Use of Cryptographic Control*)</u>** Kriptografi merangkumi kaedah-kaedah seperti yang berikut: a) **Enkripsi** Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (*encryption*); dan b) **Tandatangan Digital** Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan.	Pentadbir Sistem
8.24.2	**<u>Pengurusan Kunci Awam (*Public Key Management*)</u>** Pengurusan ke atas Pengurusan Infrastruktur Kunci Awam/*Public Key Infrastructure* (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi	Pentadbir Sistem

	kunci berkenaan daripada diubah, di musnah dan didedahkan sepanjang tempoh sah kunci tersebut.	
8.25 Kitar Hayat Pembangunan Sistem yang Selamat (*Secure Development Life Cycle*)		
ID	**PENERANGAN**	**PERANAN**
8.25.1	**<u>Dasar Pembangunan Sistem yang Selamat (*Secure Development Policy*)</u>** Peraturan untuk pembangunan sistem hendaklah diwujudkan dan digunakan selaras dengan perkembangan dan perubahan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti berikut : a) Keselamatan persekitaran pembangunan meliputi proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang telah diberi kuasa dan mengikut prosedur yang telah ditetapkan; b) Keperluan keselamatan dalam fasa reka bentuk sistem dan pangkalan data; c) Mengadakan titik semakan keselamatan di dalam jadual perbatuan projek pembangunan sistem maklumat; d) Kod atau aturcara program yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; dan e) Bagi pembangunan secara penyumberluaran (*outsource*), pembekal yang dilantik mestilah berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.	Pembangun Sistem Pentadbir Sistem

8.25.2	**<u>Kitar Hayat Pembangunan Sistem yang Selamat (*Secure Development Life Cycle*)</u>** Kementerian hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. Kementerian perlu melaksanakan penilaian 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.	Pembangun Sistem Pentadbir Sistem

8.26 Keperluan Keselamatan Aplikasi (*Application Security Requirements)*		
ID	**PENERANGAN**	**PERANAN**
8.26.1	**<u>Melindungi Perkhidmatan Aplikasi dalam Rangkaian Awam (*Securing Application Services on Public Networks*)</u>** Maklumat aplikasi yang melalui rangkaian umum (*public networks*) hendaklah dilindungi daripada aktiviti penipuan dan pendedahan maklumat yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti berikut : a) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (*authentication*); b) Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi; c) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan d) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	Pentadbir Sistem
8.26.2	**<u>Melindungi Transaksi Perkhidmatan Aplikasi (*Protecting Application Services Transactions*)</u>** 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	Pentadbir Sistem Pemilik Sistem

	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; iv. Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi; dan v. Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh Kerajaan.	
8.26.3	**<u>Keperluan Keselamatan Aplikasi (*Application Security Requirements*)</u>** Spesifikasi reka bentuk perlu mengandungi keperluan keselamatan sistem maklumat. Sekiranya sesuatu produk *off-the-shelf* diperoleh, pembekal perlu dimaklumkan berkenaan keperluan keselamatan.	Pentadbir Sistem Pemilik Sistem
8.27 Prinsip Reka Bentuk dan Kejuruteraan Sistem yang Selamat (*Secure System Architecture and Engineering Principles*)		
ID	**PENERANGAN**	**PERANAN**
8.27.1	**<u>Prinsip Kejuruteraan Sistem yang Selamat (*Secure System Engineering Principles*)</u>** Semua sistem maklumat hendaklah dibangunkan, dilaksanakan dan dikendalikan secara selamat berdasarkan prinsip kejuruteraan dan seni bina sistem selamat bagi melindungi kerahsiaan, integriti dan ketersediaan maklumat.	Pentadbir Sistem Pembangun Sistem

	Prinsip bagi kejuruteraan sistem yang keselamatan hendaklah disediakan, didokumenkan, diselenggarakan dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Antara prinsip kejuruteraan yang perlu dipertimbangkan adalah: a) Menerapkan prinsip "*zero trust*", termasuk keperluan pengesahan dan kebenaran akses berasaskan konteks (contohnya peranan dan klasifikasi data); b) Menyemak teknologi baharu memastikan kawalan keselamatan bersesuaian dilaksanakan; c) Menggunakan prinsip *defense in depth, least privilege* dan prinsip kejuruteraan keselamatan lain yang lain selari dengan keperluan semasa dan patuh peraturan yang berkuat kuasa; dan d) Menyediakan langkah kawalan seperti pemisahan perkhidmatan (seperti *containerization*), ketahanan terhadap gangguan, dan rintangan manipulasi maklumat.	
8.28 Pengekodan Selamat (*Secure Coding*)		
ID	**PENERANGAN**	**PERANAN**
8.28.1	**<u>Kawalan capaian kepada kod sumber (*Source Code*)</u>** Kawalan capaian kepada kod sumber atau atur cara program perlu dilaksanakan bagi mengelakkan kecurian, pengubahsuaian dan penghapusan tanpa kebenaran. Kod sumber bagi semua aplikasi dan perisian adalah menjadi hak milik Kementerian. Kementerian perlu memastikan amalan pengekodan	Pentadbir Sistem Pembangun Sistem

	yang selamat dalam pembangunan sistem dilaksanakan berdasarkan ancaman dan kelemahan terkini. (Rujukan: ISO/IEC 27001 & 27002)	
8.29 Pengujian dan Penerimaan Keselamatan Sistem (*Security Testing in Development and Acceptance*)		
ID	**PENERANGAN**	**PERANAN**
8.29.1	**<u>Pengujian Keselamatan Sistem (*System Security Testing*)</u>** 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 mengenal pasti kesilapan maklumat; c) menjalankan proses semak dan pengesahan ke atas *output* data daripada setiap proses aplikasi untuk menjamin ketepatan; d) melakukan pengimbasan kelemahan untuk mengenal pasti konfigurasi yang tidak selamat dan kelemahan sistem; e) menjalankan ujian penembusan untuk mengenal pasti kod dan reka bentuk yang tidak selamat; dan f) melaksanakan pengujian keselamatan sistem berdasarkan dokumen ISO/IEC/IEEE 29119-1:2022 *Software Testing Standard* serta garis panduan pengujian keselamatan dan sistem yang sedang berkuat kuasa.	Pentadbir Sistem Pemilik Sistem

8.29.2	**<u>Pengujian Penerimaan Sistem (*System Accepting Testing*)</u>** 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) pengujian penerimaan sistem hendaklah merangkumi keperluan keselamatan sistem maklumat dan kepatuhan kepada polisi pembangunan selamat; b) penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem diguna pakai; dan c) pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan (*vulnerability assessment*).	Pentadbir Sistem Pemilik Sistem

8.30 Pembangunan oleh Pembekal (*Outsourced Development*)		
ID	**PENERANGAN**	**PERANAN**
8.30.1	**<u>Pembangunan oleh Khidmat Luaran (*Outsourced Software Development*)</u>** Pembangunan sistem secara *outsource* perlu sentiasa dikawal selia dan dipantau oleh pemilik sistem dan juga perlu mematuhi perkara-perkara seperti berikut: a) Kod sumber bagi semua aplikasi dan perisian adalah menjadi **HAK MILIK KKDW** kecuali bagi jenis aplikasi *Commercial Off-The-Shelf* (COTS); b) Bagi semua perkhidmatan sumber luaran, *Software as a Service* (*SaaS*) yang mengendalikan Maklumat	Pentadbir Sistem Pemilik Sistem

	Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori **"KKDW berhak mencapai kod sumber dan data/maklumat dan KKDW berhak melaksanakan pengolahan risiko ke atas aplikasi/sistem ICT yang dibangunkan"**; c) Memastikan sistem ICT yang disediakan kepada Kementerian sentiasa dalam keadaan selamat dan dilindungi dengan mengambil kira keselamatan data-dalam-simpanan (*data-at-rest*), data-dalam-pergerakan (*data-in-motion*) dan data-dalam-penggunaan (*data-in-use*); d) Dokumen kontrak bagi tujuan pengurusan *outsourcing* perlu merangkumi pengakuan kerahsiaan dan integriti maklumat jabatan oleh pihak pembekal/perunding. Pelanggaran perjanjian boleh dikenakan tindakan undang-undang yang berkaitan; e) *Intellectual property rights* (IPR) aplikasi dan perisian yang dibangunkan oleh pihak ketiga kepada Kementerian adalah hak milik Kementerian; f) Adalah amat digalakkan dalam sepanjang tempoh fasa pembangunan aplikasi/sistem ICT, kos penyenggaraan bagi lesen perisian ditanggung oleh pihak pembekal. Perkara ini perlu dipersetujui secara bersama dan boleh dinyatakan dalam klausa kontrak projek; dan g) Pembekal yang dilantik perlu berkebolehan untuk mengenal pasti dan menambah baik kelemahan aspek keselamatan semasa fasa pembangunan sistem.	

8.31 Pengasingan Persekitaran Pembangunan, Pengujian dan Pengeluaran (*Separation of Development, Test and Production Environments*)		
ID	**PENERANGAN**	**PERANAN**
8.31.1	**<u>Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi (*Separation of Development, Test and Operational Facilities*)</u>** Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Perkakasan dan perisian yang digunakan bagi tugas mentakrifkan, mendokumentasikan, membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai produksi (*production*); b) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; c) Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat; d) menguji perubahan kepada sistem pengeluaran dan aplikasi dalam persekitaran ujian atau persekitaran sementara; e) tidak menguji dalam persekitaran produksi kecuali dalam keadaan yang telah ditentukan dan diluluskan; f) penyusun, editor dan alat pembangunan atau program utiliti lain yang tidak boleh diakses daripada sistem pengeluaran apabila tidak diperlukan; dan	Pentadbir Sistem

	g) memaparkan label pengenalan persekitaran yang sesuai dalam menu untuk mengurangkan risiko ralat.	
8.31.2	**<u>Persekitaran Pembangunan Selamat (*Secure Development Environment*)</u>** Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. Kementerian 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 Pembangun Sistem

8.32 Pengurusan Perubahan (*Change Management*)		
ID	**PENERANGAN**	**PERANAN**
8.32.1	**<u>Pengurusan Perubahan (*Change Management*)</u>** Perubahan dalam Kementerian, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara berikut: a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkodkan dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja.	Pentadbir Sistem Pemilik Sistem Pengguna Aset

8.32.2	**<u>Prosedur Kawalan Perubahan Sistem (*System Change Control Procedures*)</u>** Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perkara yang perlu dipatuhi adalah seperti yang 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 Kementerian. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal; c) mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja; dan d) capaian kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.	Pentadbir Sistem
8.32.3	**<u>Kajian Semula Keperluan Teknikal bagi Aplikasi Selepas Perubahan Platform Operasi (*Technical Review of Applications After Operating Platform Change*)</u>** Apabila platform operasi berubah, aplikasi penting perniagaan hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau	Pentadbir Sistem

	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 Kementerian dan Pelan Pengurusan Keselamatan Maklumat sistem tersebut.	
8.32.4	**<u>Sekatan ke atas Perubahan Dalam Pakej Perisian (*Restrictions on Changes to Software Packages*)</u>** Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.	Pentadbir Sistem
8.33 Data Pengujian (*Test Information*)		
ID	**PENERANGAN**	**PERANAN**
8.33.1	**<u>Perlindungan Data Ujian (*Protection of Test Data*)</u>** Untuk memastikan perlindungan ke atas maklumat yang digunakan untuk pengujian, 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;	Pemilik Sistem Pentadbir Sistem

	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 dipadamkan sebaik sahaja pengujian selesai; d) Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar; e) Melindungi maklumat sensitif melalui penyingkiran atau pengaburan data jika digunakan untuk ujian; dan f) Memadam maklumat operasi daripada persekitaran ujian serta-merta dengan betul selepas ujian selesai untuk mengelakkan penggunaan maklumat ujian tanpa kebenaran.	

8.34 Perlindungan Sistem Maklumat Semasa Pengujian Audit (*Protection of Information Systems During Audit Testing*)		
ID	**PENERANGAN**	**PERANAN**
8.34.1	**<u>Kawalan Audit Sistem Maklumat (*Information Systems Audit Controls*)</u>** Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses perniagaan. Garis panduan berikut harus dipatuhi: a) bersetuju dengan permintaan audit untuk akses kepada sistem dan data dengan pengurusan yang sesuai; b) bersetuju dan mengawal skop ujian audit teknikal;	Pemilik Sistem Pentadbir Sistem

	c) mengehadkan ujian audit kepada akses baca sahaja kepada perisian dan data. Jika akses baca sahaja tidak tersedia untuk mendapatkan maklumat yang diperlukan, pengujian perlulah dilaksanakan oleh pentadbir berpengalaman yang mempunyai hak akses yang diperlukan bagi pihak juruaudit; d) jika akses diberikan keperluan keselamatan bagi peranti yang digunakan untuk mengakses sistem perlulah ditetapkan dan disahkan terlebih dahulu sebelum atau akses dibenarkan; e) hanya membenarkan akses selain daripada baca sahaja untuk salinan terpencil fail sistem, memadamkannya apabila audit selesai atau memberi mereka perlindungan yang sewajarnya jika terdapat kewajiban untuk menyimpan fail tersebut di bawah keperluan dokumentasi audit; f) mengenal pasti dan bersetuju dengan permintaan untuk pemprosesan khas atau tambahan, seperti menjalankan alat audit; g) menjalankan ujian audit yang boleh menjejaskan ketersediaan sistem di luar waktu operasi; dan h) memantau dan mengelog semua akses untuk tujuan audit dan ujian.	

#9 LAMPIRAN



LAMPIRAN A

AKUAN PEMATUHAN POLISI KESELAMATAN SIBER (WARGA KKDW)



AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
KEMENTERIAN KEMAJUAN DESA DAN WILAYAH
(WARGA KKDW)

Nama : .....

No. Kad Pengenalan :.....

Jawatan :.....

Bahagian/Unit :.....

No. Telefon Pejabat/ Bimbit :.....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :

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

Tandatangan :.....

Tarikh :.....

Disahkan oleh,

.....

Pegawai Keselamatan ICT (ICTSO)

b/p Ketua Setiausaha

Kementerian Kemajuan Desa dan Wilayah

Tarikh :.....

LAMPIRAN B

AKUAN PEMATUHAN POLISI KESELAMATAN SIBER (KONTRAKTOR / PEMBEKAL)



AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
KEMENTERIAN KEMAJUAN DESA DAN WILAYAH
(KONTRAKTOR / PEMBEKAL)

Nama : .....

No. Kad Pengenalan :.....

Jawatan :.....

No. Telefon Pejabat/ Bimbit :.....

Nama Syarikat :.....

No. Pendaftaran Syarikat :.....

Nama Projek :.....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :

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

Tandatangan :.....

Tarikh :.....

Disahkan oleh,

.....

Pegawai Keselamatan ICT (ICTSO)

b/p Ketua Setiausaha

Kementerian Kemajuan Desa dan Wilayah

Tarikh :.....

LAMPIRAN C

UNDANG-UNDANG DAN DASAR YANG TERPAKAI

Arahan Pentadbiran Ketua Pengarah MAMPU Bilangan 1 Tahun 2019 ini hendaklah dibaca bersama dengan akta-akta, warta, pekeliling-pekeliling, surat pekeliling dan peraturan dalaman yang berkaitan dan sedang berkuat kuasa antaranya seperti berikut;

1. Arahan Keselamatan;
2. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan"
3. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS)
4. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi- Agensi Kerajaan";
5. Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022;
6. Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024;
7. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama)- "Tatacara Penyediaan, Penilaian dan Penerimaan Tender";
8. Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024
9. SuratPekeliling Perbendaharaan Bil. 3/1995 - "Peraturan Perolehan Perkhidmatan Perundingan";
10. Akta Tandatangan Digital 1997;
11. Akta Rahsia Rasmi 1972;
12. Akta Jenayah Komputer 1997;
13. Akta Hak Cipta (Pindaan) Tahun 1997;
14. Akta Komunikasi dan Multimedia 1998;
15. Perintah-Perintah Am;
16. Arahan Perbendaharaan;

17. Arahan Teknologi Maklumat 2007;
18. Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk "Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam";
19. Etika Penggunaan E-mel dan Internet MAMPU;
20. MyPortfolio;
21. Pelan Kesinambungan Perkhidmatan KKDW;
22. Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 bertajuk "Penggunaan Media Jaringan Sosial di Sektor Awam";
23. Pekeliling Perbendaharaan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan (TPA)";
24. Pekeliling Perkhidmatan Bil 5 2007 bertajuk "Panduan Pengurusan Pejabat bertarikh 30 April 2007";
25. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), April 2016;
26. Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bilangan 3 Tahun 2015 “Dasar Perkhidmatan GPKI” ;
27. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 "Langkah-langkah mengenai penggunaan Mel Elektronik Agensi- Agensi Kerajaan", Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan Government Unified Communication (MyGovUC);
28. Akta Keselamatan Siber 2024 (Akta 854);
29. Surat Pekeliling Am Bil. 4 Tahun 2024: Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
30. PKPA Bil 3 Tahun 2015: Dasar Perkhidmatan GPKI;
31. ISO/IEC/IEEE 29119-1:2022 Software Testing Standard;
32. Dasar Kriptografi Negara;
33. Akta Tandatangan Digital 1997;
34. Akta Kerajaan Elektronik 2007;
35. Surat Pekeliling Am Bil. 4 Tahun 2022: Garis Panduan Sanitasi Media Elektronik; dan
36. Pekeliling Am Bil. 1 Tahun 2025: Garis Panduan Pengurusan Kesinambungan Perkhidmatan dalam Perkhidmatan Awam.