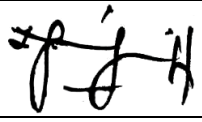
MAJLIS PERBANDARAN PEKAN BANDAR DIRAJA

POLISI KESELAMATAN SIBER

PMPPBDR.PKS.01

	DISEDIAKAN OLEH	DISEMAK OLEH	DILULUSKAN OLEH
TANDATANGAN			
NAMA	JAMAIAH BINTI AHMAD	TPr ZURAIDAH BINTI ABDUL MAJID	MOHAMAD NASIR BIN JUSOH, AAP.
JAWATAN	PEN. PEGAWAI TEKNOLOGI MAKLUMAT	SETIAUSAHA	YANG DIPERTUA
TARIKH	01.06.2025	01.06.2025	01.06.2025

PEMEGANG DOKUMEN
KETUA BAHAGIAN TEKNOLOGI MAKLUMAT

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**2/114**

REKOD PINDAAN

TARIKH PINDAAN	NO. PINDAAN /NO. KELUARAN	RUJUKAN PINDAAN/ MUKASURAT TERLIBAT	BUTIR-BUTIR PINDAAN	DILULUSKAN OLEH
01.06.2025	00/03	1-112	Perubahan kepada Polisi Keselamatan Siber	Yang Dipertua
	00/03	1-112	Perubahan nama jabatan kepada Majlis Perbandaran Pekan Bandar Diraja	Yang Dipertua

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	3/114

KANDUNGAN

TAKRIFAN..... **8**

TUJUAN..... **11**

LATAR BELAKANG..... **11**

OBJEKTIF..... **11**

TADBIR URUS..... **12**

CARTA STRUKTUR ORGANISASI SPKM MPPBDR..... **13**

PERANAN DAN TANGGUNGJAWAB JAWATANKUASA SPKM..... **14**

ASET ICT MPPBDR..... **15**

RISIKO..... **19**

PRINSIP KESELAMATAN..... **22**

TEKNOLOGI..... **29**

PROSES..... **34**

MANUSIA..... **37**

PELAN PENGURUSAN KESELAMATAN MAKLUMAT..... **40**

A1 KAWALAN POLISI KESELAMATAN MAKLUMAT *(INFORMATION SECURITY POLICY CONTROLS)*... **42**

5.0 KAWALAN ORGANISASI *(ORGANIZATIONAL CONTROL)*..... **42**

5.1 POLISI KESELAMATAN MAKLUMAT *(POLICIES FOR INFORMATION SECURITY)*..... **42**

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBITIES)*..... **43**

5.3 PENGASINGAN TUGAS *(SEGREGATION OF DUTIES)*..... **48**

5.4 TANGGUNGJAWAB PENGURUSAN *(MANAGEMENT RESPONSIBILITIES)*..... **48**

5.5 HUBUNGAN DENGAN PIHAK BERKUASA *(CONTACT WITH AUTHORITIES)*..... **48**

5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS *(CONTACT WITH SPECIAL INTEREST GROUPS)* **49**

5.7 ANCAMAN PERISIKAN *(THREAT INTELLIGENCE)* **49**

5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK *(INFORMATION SECURITY IN PROJECT MANAGEMENT)* **50**

5.9 MAKLUMAT INVENTORI ASET DAN YANG BERKAITAN *(INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS)* **50**

5.10 MAKLUMAT PENGGUNAAN ASET YANG BOLEH DITERIMA DAN YANG BERKAITAN *(ACCEPTABLE USE OF INFORMATION AND OTHER ASSOCIATED ASSETS)* **51**

5.11 PEMULANGAN ASET *(RETURN OF ASSETS)* **51**

5.12 PENGELASAN MAKLUMAT *(CLASSIFICATION OF INFORMATION)* **51**

5.13 PELABELAN MAKLUMAT *(LABELLING OF INFORMATION)* **52**

5.14 PEMINDAHAN MAKLUMAT *(INFORMATION TRANSFER)* **52**

5.15 KAWALAN AKSES *(ACCESS CONTROL)* **54**

5.16 PENGURUSAN IDENTITI *(IDENTITY MANAGEMENT)* **60**

5.17 MAKLUMAT PENGESAHAN (AUTHENTICATION INFORMATION) **61**

5.18 HAK AKSES *(ACCESS RIGHT)* **61**

5.19 HUBUNGAN KESELAMATAN MAKLUMAT DENGAN PEMBEKAL *(INFORMATION SECURITY IN SUPPLIER RELATIONSHP)* **62**

5.20 PERJANJIAN KESELAMATAN MAKLUMAT DENGAN PEMBEKAL *(ADDRESSING INFORMATION SECURITY WITHIN SUPPLIER AGREEMENTS)* **63**

5.21 PENGURUSAN KESELAMATAN MAKLUMAT DALAM RANTAIAN KOMUNIKASI MAKLUMAT ICT *(MANAGING INFORMATION SECURITY IN THE INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SUPPLY CHAIN)* **63**

5.22 PEMANTAUAN, SEMAKAN DAN PERUBAHAN PENGURUSAN PERKHIDMATAN PEMBEKAL *(MONITORING, REVIEW AND CHANGE MANAGEMENT OF SUPPLIER SERVICES)* **64**

5.23 KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN AWAN *(INFORMATION SECURITY FOR USE OF CLOUD SERVICES)* **65**

5.24 PERANCANGAN, PENYEDIAAN DAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY INCIDENT MANAGEMENT PLANNING AND PREPARATION)* **66**

5.25 PENILAIAN DAN KEPUTUSAN PERISTIWA KESELAMATAN MAKLUMAT *(ASSESSMENT AND DECISION ON INFORMATION SECURITY EVENTS)* **66**

5.26 MAKLUMBALAS INSIDEN KESELAMATAN MAKLUMAT *(RESPON TO INFORMATION SECURITY INCIDENT)* **66**

5.27 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT *(LEARNING FORMINFORMATION SECURITY INCIDENTS)* **67**

5.28 PENGUMPULAN BUKTI *(COLLECTION OF EVIDENCE)* **67**

5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN (INFORMATION SECURITY DURING DISRUPTION) 68
5.30 KETERSEDIAAN ICT UNTUK KESINAMBUNGAN PERKHIDMATAN (ICT READINESS FOR BUSINESS CONTINUITY) 70
5.31 UNDANG-UNDANG, BERKANUN, PERATURAN DAN KEPERLUAN KONTRAK (LEGAL, STATUTORY, REGULATORY AND CONRACTUAL REQUIREMENTS) 72
5.32 HAK HARTA INTELEK (INTELLECTUAL PROPERTY RIGHTS) 74
5.33 PERLINDUNGAN REKOD *(PROTECTION OF RECORDS)* 74
5.34 PRIVASI DAN PERLINDUNGAN MAKLUMAT PENGELANAN PERIBADI *(PRIVACY AND PROTECTION OF PERSONAL IDENTIFIABLE INFORMATION (PII))* 74
5.35 KAJIAN KEBEBASAN KESELAMATAN MAKLUMAT *(INDEPENDENT REVIEW OF INFORMATION SECURITY)* 75
5.36 PEMATUHAN POLISI, PERATURAN DAN PIAWAIAN KESELAMATAN MAKLUMAT *(COMPLIANCE WITH POLICIES, RULES AND STANDARD FOR INFORMATION SECURITY)* ... 75
5.37 PROSEDUR OPERASI YANG DIDOKUMENKAN *(DOCUMENTED OPERATING PROCEDURE)* 76

6.0 KAWALAN MANUSIA *(PEOPLE CONTROL)* 77

6.1 PEMERIKSAAN (SCREENING) 77
6.2 TERMA DAN SYARAT PEKERJAAN *(TERMS AND CONDITION EMPLOYMENT)* 77
6.3 KESEDARAN KESELAMATAN MAKLUMAT, PENDIDIKAN DAN LATIHAN *(INFORMATION SECURITY AWARENESS AND TRAINING)* 77
6.4 PROSES DISIPLIN *(DISCIPLINARY PROCESS)* 77
6.5 TANGGUNGJAWAB SELEPAS PENAMATAN ATAU PERUBAHAN PEKERJAAN (RESPONSIBILITIES AFTER TERMINATION OR CHANGE OF EMPLOYMENT) 78
6.6 KERAHSIAAN ATAU PERJANJIAN BUKAN PENDEDAHAN (CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS) 78
6.7 KERJA JAUH *(REMOTE WORKING)* 79
6.8 PELAPORAN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY EVENT REPORTING)* .. 79

7.0 KAWALAN FIZIKAL *(PHYSICAL CONTROL)* 80

7.1 PERIMETER KESELAMATAN FIZIKAL *(PHYSICAL SECURITY PERIMETERS)* 80
7.2 PHYSICAL ENTRY *(KEMASUKAN FIZIKAL)* 80
7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN *(SECURING OFFICES, ROOMS AND FACILITIES)* 81
7.4 PEMANTAUAN KESELAMATAN FIZIKAL *(PHYSICAL SECURITY MONITORING)* 81

7.5 PERLINDUNGAN FIZIKAL DAN ANCAMAN PERSEKITARAN *(PROTECTION AGAINST PHYSICAL AND ENVIRONMENTAL THREATS)* **82**
7.6 BEKERJA DI KAWASAN YANG SELAMAT *(WORKING IN SECURE AREA)* **83**
7.7 DASAR MEJA KOSONG DAN SKRIN KOSONG *(CLEAR DESK AND CLEAR SCREEN)* **84**
7.8 LOKASI DAN PERLINDUNGAN PERALATAN *(EQUIPMENT SITING AND PROTECTION)* **84**
7.9 KESELAMATAN ASET DI LUAR PREMIS *(SECURITY OF ASSETS OF PREMISES)* **86**
7.10 MEDIA STORAN *(STORAGE MEDIA)* **86**
7.11 UTILITI SOKONGAN *(SUPPORTING UTILITIES)* **87**
7.12 KESELAMATAN KABEL *(CABLING SECURITY)* **87**
7.13 PENYELENGGARAAN PERKAKASAN *(EQUIPMENT MAINTENANCE)* **88**
7.14 PELUPUSAN SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN *(SECURE DISPOSAL OR RE-USE OF EQUIPMENT)* **88**

8.0 KAWALAN TEKNOLOGI *(TECHNOLOGICAL CONTROL)* **91**
8.1 PERANTI AKHIR PENGGUNA *(USER END POINT DEVICES)* **91**
8.2 HAK AKSES ISTIMEWA *(PRIVILEGED ACCESS RIGHT)* **91**
8.3 SEKATAN AKSES MAKLUMAT *(INFORMATION ACCESS RESTRICTION)* **93**
8.4 AKSES KEPADA KOD SUMBER *(ACCESS TO SOURCE CODE)* **93**
8.5 PENGESAHAN KESELAMATAN *(SECURE AUTHENTICATION)* **94**
8.6 PENGURUSAN KAPASITI *(CAPACITY MANAGEMENT)* **94**
8.7 PERLIDUNGAN TERHADAP PERISIAN *MALWARE (PROTECTION AGAINST MALWARE)* **95**
8.8 PENGURUSAN KELEMAHAN TEKNIKAL *(MANAGEMENT OF TECHNICAL VULNERABILITIES)* **95**
8.9 PENGURUSAN KONFIGURASI *(CONFIGURATION MANAGEMENT)* **96**
8.10 PEMADAMAN MAKLUMAT *(INFORMATION DELETION)* **96**
8.11 DATA MASKING *(DATA MASKING)* **97**
8.12 PENCEGAHAN KEBOCORAN DATA *(DATA LEAKAGE PREVENTION)* **97**
8.13 SANDARAN MAKLUMAT *(INFORMATION BACKUP)* **98**
8.14 KEMUDAHAN PEMPROSESAN MAKLUMAT YANG BERTINDIH *(REDUNDANCY OF INFORMATION PROCESSING FACILITIES)* **99**
8.15 LOGGING *(LOGGING)* **99**
8.16 AKTIVITI PEMANTAUAN *(MONITORING ACTIVITIES)* **100**

8.17 PENYERAGAMAN JAM *(CLOCK SYNCHRONISATION)* **100**

8.18 KEISTIMEWAAN PENGGUNAAN UITILITI PROGRAM *(USE OF PRIVILEGED UTILITY PROGRAMS)* **100**

8.19 PEMASANGAN PERISIAN PADA SISTEM OPERASI *(INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS)* **101**

8.20 KESELAMATAN RANGKAIAN *(NETWORKS SECURITY)* **102**

8.21 KESELAMATAN PERKHIDMATAN RANGKAIAN *(SECURITY OF NETWORK SERVICES)* **103**

8.22 PENGASINGAN RANGKAIAN *(SEGREGATION OF NETWORKS)* **103**

8.23 TAPISAN LAMAN WEB *(WEB FILTERING)* **103**

8.24 PENGGUNAAN KIPTOGRAFI *(USE OF CRYPTOGRAPHY)* **104**

8.25 KITARAN HIDUP PEMBANGUNAN SELAMAT *(SECURE DEVELOPMENT LIFE CYCLE)* **104**

8.26 KEPERLUAN KESELAMATAN PERMOHONAN *(APPLICATION SECURITY REQUIREMENTS)* **104**

8.27 SENIBINA SISTEM SELAMAT DAN PRINSIP KEJURUTERAAN *(SECURE SYSTEM ARCHITECTURES AND ENGINEERING PRINCIPLES)* **105**

8.28 PENGEKODAN SELAMAT *(SECURE CODING)* **105**

8.29 UJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN *(SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE)* **106**

8.30 PEMBANGUNAN SUMBER LUAR *(OUTSOURCED DEVELOPMENT)* **107**

8.31 PERSEKITARAN PEMBANGUNAN PERISIAN, PENGUJIAN DAN PENGELUARAN *(SEPARATION OF DEVELOPMENT, TEST AND PRODUCTION ENVIRONMENT)* **107**

8.32 PENGURUSAN PERUBAHAN *(CHANGE MANAGEMENT)* **107**

8.33 MAKLUMAT UJIAN *(TEST INFORMATION)* **108**

8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PENGUJIAN AUDIT *(PROTECTION OF INFORMATION SYSTEMS DURING AUDIT TESTING)* **108**

GLOSARI **110**

LAMPIRAN 1 : AKUJANJI KESELAMATAN MAKLUMAT MPPBDR **113**

LAMPIRAN 2 : DASAR KESELAMARAN SISTEM KESELAMATAN MAKLUMAT (SPKM) **114**

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**8/114**

TAKRIFAN

1.	Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk, flash disk,* CDROM untuk sebarang kemungkinan adanya 'virus.
2.	Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
3.	Aset Alih	Aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
4.	Backup (Sandaran)	Proses penduaan sesuatu dokumen atau maklumat.
5.	Baki risiko	Risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan.
6.	*Bandwidth*	Jalur lebar - Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
7.	BCP/PKP	Business Continuity Planning Pelan Kesinambungan Perkhidmatan
8.	CCTV	Closed-Circuit Television System - Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera videodipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
9.	CIA	*Confidentiality, Integrity, Availability*
10.	CDO	*Chief Digital Officer* - Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan maklumat digitalbagi menyokong arah tuju sesebuah organisasi.

11.	*Clear Desk* dan *Clear Screen*	Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
12.	Denial of service	Halangan pemberian perkhidmatan
13.	Defence-in-depth	Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.
14.	Downloading	Aktiviti muat turun sesuatu perisian.
15.	Encryption	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yangsah.
16.	Escrow (eskrow)	Sebarang sistem yang membuat salinan kunci penyulitan supaya boleh dicapai oleh individu yang dibenarkan pada bila-bila masa.
17.	*Forgery*	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
18.	CERT MPPBDR	*Computer Emergency Response Teams* atau Pasukan Tindak Balas Keselamatan Siber MPPBDR.
19.	*Hard disk*	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebihpantas.
20.	*Hub*	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu port kepada semua *port* yang lain.
21.	*ICT*	*Information and Communication Technology* - Teknologi Maklumat dan Komunikasi
22.	*ICTSO*	*ICT Security Officer* - Pegawai yang bertanggungjawab terhadap keselamatan siber.

23.	Impak teknikal	Melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti.
24.	BTM	Bahagian Teknologi Maklumat
25.	JKP	Jabatan Khidmat Pengurusan

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**11/114**

TUJUAN

Polisi Keselamatan Siber MPPBDR ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh kakitangan MPPBDR, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MPPBDR dalam melindungi maklumat di ruang siber.

LATAR BELAKANG

Polisi Keselamatan Siber MPPBDR mengandungi peraturan-peraturan mengenai penggunaan perkakasan dan perisian (aset) teknologi maklumat dan komunikasi (ICT) MPPBDR. Peraturan-peraturan ini perlu difahami dan dipatuhi oleh semua pengguna di MPPBDR. Dasar ini juga menerangkan mengenai tanggungjawab dan peranan pengguna dalam melindungi aset ICT MPPBDR.

OBJEKTIF

Polisi Keselamatan Siber MPPBDR diwujudkan untuk mencapai tahap keselamatan ICT yang menyeluruh bagi memastikan kesinambungan serta perkongsian maklumat dalam semua urusan di MPPBDR dengan melindungi kepentingan Majlis dan meminimumkan insiden keselamatan ICT serta kesannya seperti berikut;

a. Memastikan kelancaran operasi MPPBDR dan meminimumkan kerosakan atau kemusnahan;
b. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;

c. Mencegah salah guna atau kecurian aset ICT Kerajaan;
d. Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;
e. Meningkatkan tahap keselamatan ICT kepada para kakitangan, pengguna dan pembekal;
f. Memperkemaskan pengurusan risiko; dan
g. Melindungi aset ICT daripada penyelewengan oleh kakitangan, pengguna dan pembekal.

TADBIR URUS

Bagi memastikan keberkesanan dan kejayaan pelaksanaan PKS MPPBDR, satu (1) struktur tadbir urus iaitu Jawatankuasa Sistem Pengurusan Keselamatan Maklumat (SPKM) MPPBDR telah diwujudkan seperti berikut:

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	13/114

CARTA STRUKTUR ORGANISASI SPKM MPPBDR

PENASIHAT
Tn. Mohamad Nasir bin Jusoh, AAP
Yang Dipertua

KETUA AUDIT DALAM
Pn. Samsuriyati binti Uyob
Ketua Bah. Akaun dan Hasil

CIO/ PENGERUSI / WAKIL PENGURUSAN ISO
Pn. TPr Zuraidah binti Abdul Majid
Setiausaha

PROJECT MANAGER/ PENYELARAS ISO
Pn. Jamaiah binti Ahmad
Ketua Bah. Teknologi Maklumat

URUSETIA AUDIT DALAM
Pn. Alina binti Daud

TEAM LEADER
Pn. Nor Fazliana binti Abu Bakar
Ketua Jab. Perbendaharaan

DEPUTY TEAM LEADER
Pn. Nurul Azma binti Muhammad
Ketua Jab. Perkhidmatan Perbandaran

PELAKSANA SPKM

JURUAUDIT DALAM SPKM

Jab. Perhubungan Awam dan Komuniti
1. En. Mohd Khairul Azlan bin Omar

Jab. Kejuruteraan
2. En. Mohd Habbullah bin Abu Bakar
3. En. Samsul Azwan bin Mohd Soaud
4. En. Ibrahim bin Hashim
5. En. Ahmad Amira bin Amirudin
6. En. Mohd Firdaus bin Ramli
7. En. Muhammad Amir Shahril bin Ahmad Rizal
8. En. Ahmad Solihin bin Mohd Nor
9. En. Herryyandi bin Abdul Gafar

Bah. Landskap dan Rekreasi
10. En. Ahmad Azizul Rahim bin Ahmad Abdul Aziz
11. En. Muhammad Iqbal Fahim bin Rozlan

Bah. Undang-Undang
12. En. Sheikh Ahmad Norqamarul Haeizzack bin Sh Nor Hasmadi

Bah. Pusat Setempat (OSC)
13. Pn. Nor Faridah Hanom bin Mohamed
14. En. Ifwat Haidhar bin Ibrahim

Bah. Ukur Bahan
15. En. Wan Armizi bin Wan Abdullah

Bah. Integriti dan Audit Dalam
16. En. Abdul Latif Ariff bin Shamsul Amri

SKOP UTAMA

Jab. Perkhidmatan Perbandaran
1. Pn. Noridura binti Ismail
2. En. Mohd Khairul Hafiz bin Abdul Kahar

Jab. Penilaian dan Pengurusan Harta
3. En. Mohd Azuan bin Othman
4. Cik Asma' binti Abdul Razak
5. Pn. Engku Rahayu Asikin bin Eg. Ibrahim

SKOP SOKONGAN

Bah. Teknologi Maklumat
6. En. Muhamad Iqbal Zahin bin Hashim
7. En. Saiful Shahiruddin bin Mohammad
8. Pn. Norazlin binti Dzulkarnain
9. En. Amin Khaydatul Adam bin Abdul Rahim

Bah. Sumber Manusia
10. Pn. Nor Lida binti Mohd Hashim
11. Pn. Nor Zurina binti Abdullah

Bah. Perolehan dan Stor
12. En. Khairul Hisham bin Bukhari

Bah. Akaun dan Hasil
13. Pn. Samsuriyati binti Uyob

Bah. Penguatkuasaan dan Tempat Letak Kereta
14. En. Muhammad Shazwan bin Abdul Musalleb

Bah. Penyelenggaraan & Infra
15. En. Nasrul Arif bin Ahmad
16. En. Khairul Anuwar bin Muhammad

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	14/114

PERANAN DAN TANGGUNGJAWAB JAWATANKUASA SPKM

Rujuk kepada PMPPBDR.PSPB.01 – 5.3.1 Peranan dan Tanggungjawab

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	15/114

ASET ICT MPPBDR

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

a. Maklumat

i. Semua penyedia perkhidmatan dalam MPPBDR hendaklah mengenai pasti maklumat yang dijana dan hendaklah mengasingkannya mengikut kategori:

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

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

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

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

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

b. Aliran Data

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

1. Saluran komunikasi dan aliran data antara sistem di MPPBDR;
2. Saluran komunikasi dan aliran data ke sistem luar; dan
3. Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan di anggap sebagai saluran komunikasi luaran.

c. Platform Aplikasi dan Perisian

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

d. Peranti Fizikal dan Sistem

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

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

e. Sistem Luaran

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

f. Sumber Luaran

i. Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkod dan dinilai tahap keselamatannya secara berkala. Perkhidmatan sumber luaran ialah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi MPPBDR. Contoh perkhidmatan sumber luaran ialah:

1. Perisian Sebagai Satu Perkhidmatan
2. Platform Sebagai Satu Perkhidmatan
3. Infrastruktur Sebagai Satu Perkhidmatan
4. Storan Pengkomputeran Awan
5. Pemantauan Keselamatan

ii. Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan, dikaji semula dan dipastikan keselamatannya secara berkala.

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

RISIKO

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

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

Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

a. Kerentanan

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

b. Ancaman

   Pejabat MPPBDR hendaklah mengenai pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

c. Impak

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

d. Tahap Risiko

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

e. Penguraian Risiko

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

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

1. Teknologi

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

2. Proses

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

3. Manusia

   Mengenai pasti sumber manusia berkelayakan dan kompeten yang mencukupi serta memastikan pengurusan sumber manusia dilaksanakan sebagai pengolahan risiko yang berkesan.

f. Pengurusan Risiko

1. Penyedia perkhidmatan digital di MPPBDR hendaklah memastikan tadbir urus pengurusan risiko diwujudkan dengan mengambil kira perkara berikut:
   i. mengenai pasti kerentanan;
   ii. mengenai pasti ancaman;
   iii. menilai risiko;
   iv. menentukan penguraian risiko;
   v. memantau keberkesanan penguraian risiko; dan
   vi. memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

2. Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya sekali setahun di dalam Mesyuarat Jawatankuasa Induk Pengurusan Risiko SPKM dan dimaklumkan kepada Mesyuarat Kajian Semula Pengurusan SPKM.

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**22/114**

PRINSIP KESELAMATAN

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

a. **Akses Atas Dasar Perlu Mengetahui**

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan akses di bawah prinsip ini adalah berasaskan kepada klasifikasi maklumat dan tapisan keselamatan pengguna seperti berikut (Sumber: Arahan Keselamatan perenggan 53, muka surat 15):-

i. Klasifikasi Maklumat

Keselamatan ICT Kerajaan hendaklah mematuhi "Arahan Keselamatan" perenggan 53, muka surat 15, di mana maklumat dikategorikan kepada Rahsia Besar, Rahsia, Sulit dan Terhad. Data, bahan atau maklumat rasmi yang sensitif atau bersifat terperingkat perlu dilindungi dari pendedahan, dimanipulasi atau diubah semasa dalam penghantaran. Penggunaan kod dan tandatangan digital mesti dipertimbangkan bagi melindungi data yang dikirim secara elektronik. Dasar kawalan akses ke atas aplikasi atau sistem juga hendaklah mengikut klasifikasi maklumat yang sama, iaitu sama ada rahsia besar, rahsia, sulit atau terhad; dan

ii. Tapisan Keselamatan Pengguna

Polisi Keselamatan Siber MPPBDR adalah mematuhi prinsip bahawa pengguna boleh diberi kebenaran mengakses kategori maklumat tertentu setelah siasatan latar belakang menunjukkan tiada sebab atau faktor untuk menghalang pengguna daripada berbuat demikian.

b. **Hak Akses Minimum**

Hak akses kepada pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas adalah diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu data atau maklumat. Hak akses adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

c. **Akauntabiliti**

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT MPPBDR hendaklah menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:-

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa

ke semasa;

iii. Menentukan maklumat sedia untuk digunakan;

iv. Menjaga kerahsiaan kata laluan;

v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan 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 daripada diketahui umum.

d. **Pengasingan**

i. Prinsip pengasingan bermaksud bahawa semua tugas-tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data diasingkan. Ia bertujuan untuk mengelak akses yang tidak dibenarkan dan melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat, dimanipulasi dan seterusnya, mengenalkan integriti dan kebolehsediaan; dan

ii. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. Ia bertujuan untuk mengasingkan akses kepada domain kedua-dua kumpulan tersebut seperti akses kepada fail data, fail program, kemudahan sistem dan komunikasi, manakala pemisahan antara domain pula adalah untuk mengawal dan mengurus perubahan pada konfigurasi dan keperluan sistem.

Pada tahap minimum, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut:-

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

e. **Pengauditan**

i. Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall*, dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*. Pentingnya *audit trail* ini menjadi semakin ketara apabila wujud keperluan untuk mengenal pasti punca masalah atau ancaman kepada keselamatan ICT. Oleh itu, rekod audit hendaklah dilindungi dan tersedia untuk penilaian atau tindakan serta merta;

ii. Pengauditan juga perlu dibuat ke atas rekod-rekod manual seperti dokumen operasi, nota serah tugas, kelulusan keluar pejabat, memorandum, borang kebenaran, surat kuasa, senarai inventori dan kemudahan akses log. Ini adalah kerana dalam kes-kes tertentu, dokumen ini diperlukan untuk menyokong *audit trail* sistem komputer; dan

iii. Keseluruhannya, sistem pengauditan ini adalah penting dalam menjamin akauntabiliti.

Antara lain, sistem ini dapat dirujuk bagi menentukan perkara-perkara berikut:

1. Mengesan pematuhan atau perlanggaran keselamatan;
2. Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya perlanggaran keselamatan; dan
3. Menyediakan bahan bukti bagi menentukan sama ada berlakunya perlanggaran keselamatan.

f. **Pematuhan**

Polisi Keselamatan Siber MPPBDR hendaklah dibaca, difahami dan dipatuhi. Pematuhan adalah merupakan prinsip penting dalam menghindar dan mengesan sebarang perlanggaran Dasar yang boleh membawa ancaman kepada keselamatan ICT. Pematuhan kepada Polisi Keselamatan Siber MPPBDR boleh dicapai melalui tindakan berikut:

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

dipatuhi; dan

iv. Menguatkuasakan amalan melaporkan sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan.

g. **Pemulihan**

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Antara lain, pemulihan boleh dilakukan melalui tindakan-tindakan berikut:-

i. Mewujudkan, merumuskan dan menguji Pelan Pemulihan Bencana/ kesinambungan perkhidmatan – (*Disaster Recovery Plan*/ *Business Continuity Plan*); dan

ii. Mengamalkan langkah-langkah membuat salinan data dan lain-lain amalan terbaik dalam penggunaan ICT seperti menghapuskan virus, langkah-langkah pencegahan kebakaran dan amalan *clear desk*.

h. **Saling Bergantung**

Langkah-langkah keselamatan ICT yang berkesan memerlukan pematuhan kepada semua prinsip-prinsip di atas. Setiap prinsip adalah saling lengkap melengkapi antara satu dengan lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorak sebanyak mungkin mekanisme keselamatan, dapat menjamin keselamatan yang maksimum. Prinsip saling bergantung meliputi beberapa peringkat di mana di tahap minimum,

mengandungi langkah-langkah berikut:-

i. Sambungan kepada Internet – Semua komunikasi antara sistem ICT dengan sistem luar hendaklah melalui mekanisme pusat untuk mengurus, menguatkuasa dan mengawas sebarang bahaya keselamatan. Melalui sistem ini, semua trafik dalaman hendaklah melalui *gateway firewall* yang diurus secara berpusat. Semua trafik dari luar ke dalam hendaklah juga melalui laluan ini atau melalui kumpulan modem yang dikawal secara berpusat. Dengan itu, penggunaan modem dalaman tidak dibenarkan;

ii. *Backbone* Rangkaian – *Backbone* rangkaian akan hanya mengendalikan trafik yang telah dikod untuk meminimumkan intipan;

iii. Rangkaian Jabatan – Semua rangkaian jabatan akan dihubungkan ke backbone melalui firewall yang mana akan pula mengekod semua trafik di antara rangkaian jabatan dengan rangkaian di peringkat yang seterusnya atau pusat data; dan

iv. Pelayan Jabatan – Semua data dan maklumat yang kritikal atau sensitif akan hanya disimpan di pelayan jabatan atau di pelayan yang diurus secara berpusat. Ini akan meminimumkan pendedahan, pengubahan atau kecurian. Semua data dan maklumat sensitif akan dikodkan.

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**29/114**

TEKNOLOGI

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

a. Peringkat Pemprosesan Data

1. Data-dalam-simpanan

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

   ii. Maklumat Rahsia Rasmi, Maklumat Rasmi dan PII perlu dilindungi daripada segi kerahsiaan dan integriti data. Data terbuka perlu dilindungi daripada segi integriti data.

2. Data-dalam-pergerakan

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

3. Data-dalam-penggunaan

   i. MPPBDR hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-penggunaan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Di

samping itu, teknologi untuk menentukan asal data dan tanpa sangkalan mungkin diperlukan. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data dalam penggunaan.

ii. Teknologi yang bersesuaian boleh digunakan untuk memastikan asal data dan data/transaksi tanpa-sangkal.

4. Perlindungan Ketirisan Data

i. Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.

ii. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

b. Elemen Dalam Persekitaran Pengkomputeran

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

Maklumat Terkawal hendaklah disimpan dan diproses dalam persekitaran pengkomputeran mengikut Prosedur Kawalan Keselamatan Dokumen yang dikeluarkan oleh MPPBDR.

Setiap projek ICT yang dibangunkan di MPPBDR hendaklah mempunyai Pelan Pengurusan Keselamatan Maklumat tersendiri yang mengandungi maklumat

terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

1. Peranti pengkomputeran peribadi
    i. Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, stesen kerja, telefon pintar, tablet, dan peranti storan.
    ii. Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Terkawal hendaklah memohon kebenaran daripada pihak bertanggungjawab di MPPBDR. Walau bagaimanapun, peranti pengkomputeran peribadi milik persendirian hendaklah dilarang daripada mencapai Maklumat Terkawal.

2. Peranti rangkaian
    i. Merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti suis, penghala, tembok api, peranti VPN dan kabel.
    ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**32/114**

3. Aplikasi

   i. Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi, sistem operasi.

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

4. Pelayan

   i. Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat.

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

5. Persekitaran fizikal

   i. Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.

   ii. MPPBDR hendaklah merujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.

   iii. Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko

yang dikenal pasti dan berdasarkan prinsip defence-in-depth.

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

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**34/114**

PROSES

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

a. Konfigurasi Asas
   1. Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi prasyarat pentauliahan sistem.
   2. Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan.

b. Kawalan Perubahan Konfigurasi
   1. Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.
   2. Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asas terkini.
   3. Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan.

c. Sandaran
   1. Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang sedang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan.

2. Media sandaran hendaklah disimpan dalam persekitaran yang selamat dan di lokasi yang berasingan.

d. Kitaran Pengurusan Aset

1. Pindah

i. Pemindahan hak milik aset berlaku dalam keadaan berikut:

a) Warga MPPBDR meninggalkan agensi disebabkan oleh persaraan, perletakan jawatan atau penugasan semula;

b) Aset yang dikongsi untuk kegunaan sementara;

c) Pemberian aset kepada agensi lain; dan

d) Aset dikembalikan setelah tamat tempoh sewaan.

ii. Data dalam peranti tersebut hendaklah diuruskan mengikut tatacara pelupusan di perkara (2).

2. Pelupusan

i. Pelupusan media storan hendaklah dirujuk kepada CGSO sebagai langkah pertama di mana CGSO akan membuat keputusan sama ada sistem itu mengandungi maklumat terperingkat atau sebaliknya.

ii. Berdasarkan keputusan CGSO, pelupusan perlu dirujuk kepada Arkib Negara Malaysia bagi semakan sama ada sistem itu mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara 2003 (Akta 629) dan Warta Kerajaan P.U.(A)377. Peraturan-Peraturan Arkib Negara (Penetapan Borang-Borang bagi Pelupusan Rekod Awam) 2008.

iii. Pelupusan boleh dalam bentuk pemusnahan fizikal dan/atau sanitasi data.

iv. Sanitasi data hendaklah mengikut Garis Panduan Sanitasi Media Elektronik Sektor Awam yang sedang berkuat kuasa.

3. Kitaran Hayat

   i. Kitaran hayat data hendaklah diuruskan mengikut Akta 629.

   ii. Akta 629 memberikan mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umum selama lima tahun.

MANUSIA

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

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

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

b. Kompetensi pelaksana

1. Warga MPPBDR yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.
2. Pegawai Keselamatan ICT hendaklah memenuhi syarat-syarat berikut:

   i. Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber.
   iii. Memenuhi keperluan pembelajaran berterusan.
   iv. Menimba pengalaman yang mencukupi dalam bidang keselamatan siber.
   v. Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa.

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

c. Peranan

1. Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna.
2. Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka.
3. Warga MPPBDR yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT Jabatan dikembalikan sekiranya berlaku perubahan peranan.
4. Warga MPPBDR yang terlibat dengan perubahan peranan hendaklah

menyerahkan semua aset Jabatan yang berkaitan seperti tersenarai dalam senarai aset dalam Nota Serah Tugas.

Warga MPPBDR yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan dengan diselia oleh kakitangan yang dipertanggungjawabkan oleh Jabatan

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**40/114**

PELAN PENGURUSAN KESELAMATAN MAKLUMAT

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

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

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

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

c. Tidak Boleh Disangkal
   Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal.

d. Kesahihan
   Data dan maklumat hendaklah dipastikan kesahihannya.

e. Ketersediaan

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

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

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

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**42/114**

A.1	**KAWALAN POLISI KESELAMATAN MAKLUMAT *(INFORMATION SECURITY POLICY CONTROLS)***	
5.0	**KAWALAN ORGANISASI *(ORGANIZATIONAL CONTROL)***	
5.1	**POLISI KESELAMATAN MAKLUMAT *(POLICIES FOR INFORMATION SECURITY)***	
Menerangkan hala tuju, sokongan pengurusan dan peraturan-peraturan bagi mengguna dan melindungi aset ICT selaras dengan keperluan Majlis Perbandaran Pekan dan perundangan yang berkaitan.		
5.1.1	**PELAKSANAAN DASAR**	**PERANAN**
Pelaksanaan dasar ini akan dijalankan oleh Yang Dipertua MPPBDR dibantu oleh ahli dari Mesyuarat Pengurusan yang terdiri daripada Ketua Pegawai Maklumat (CIO), semua Ketua Jabatan dan Ketua Bahagian.		**Yang Dipertua**
5.1.2	**PENYEBARAN DASAR**	**PERANAN**
Dasar ini disebarkan kepada semua pengguna MPPBDR iaitu kakitangan, pembekal, pakar runding dan lain-lain.		**Ketua Bahagian ICT, ICTSO**
5.1.3	**PENYELENGGARAAN DASAR**	**PERANAN**
Dasar ini akan disemak dan dipinda dari semasa ke semasa selaras dengan kemajuan teknologi dan perubahan pada prosedur, perundangan dan perkembangan sosial. Prosedur berhubung penyelenggaraan Polisi Keselamatan Siber MPPBDR adalah: a. Kenal pasti dan tentukan perubahan yang diperlukan; b. Kemuka cadangan pindaan untuk mendapatkan persetujuan Mesyuarat Pengurusan; c. Perubahan yang telah dipersetujui oleh mesyuarat akan dimaklumkan kepada semua pengguna; d. Dasar ini hendaklah dikaji dari masa ke masa.		**Ketua Bahagian ICT, ICTSO**
5.1.4	**PENGECUALIAN DASAR**	**PERANAN**
Polisi Keselamatan Siber MPPBDR digunapakai oleh semua pengguna ICT MPPBDR dan tiada pengecualian diberikan.		**Semua**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	43/114

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBITIES)*

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber MPPBDR.

5.2.1 YANG DIPERTUA	**PERANAN**
Peranan dan tanggungjawab Yang Dipertua adalah seperti berikut : a. Memastikan semua pengguna memahami peruntukan-peruntukan yang telah digariskan di bawah Polisi Keselamatan Siber MPPBDR; b. Memastikan semua pengguna mematuhi Polisi Keselamatan Siber MPPBDR; c. Memastikan perlindungan keselamatan adalah mencukupi dari setiap aspek; d. Memastikan program keselamatan ICT dilaksanakan.	**Yang Dipertua**
5.2.2 KETUA PEGAWAI MAKLUMAT (CIO)	**PERANAN**
Ketua Pegawai Maklumat (CIO) bagi MPPBDR ialah Setiausaha MPPBDR. Peranan dan tanggungjawab CIO adalah seperti berikut: a. Membantu Yang Dipertua dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b. Menentukan keperluan keselamatan ICT; c. Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan PKS MPPBDR serta pengurusan risiko dan pengauditan; dan d. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MPPBDR.	**Ketua Bahagian ICT, ICTSO**
5.2.3 KETUA BAHAGIAN ICT	**PERANAN**

Peranan dan tanggungjawab Ketua Bahagian ICT adalah seperti berikut: a. membantu Yang Dipertua dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MPPBDR; c. Menentukan kawalan akses pengguna terhadap aset ICT MPPBDR; d. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CIO; dan e. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MPPBDR. f. Membangun dan menyelaras pelaksanaan program mengenai keselamatan ICT. g. Koordinator Pengurusan Kesinambungan Perkhidmatan (Koordinator PKP) MPPBDR.	**Ketua Bahagian ICT**
5.2.4 PEGAWAI KESELAMATAN ICT (ICTSO)	**PERANAN**
Pegawai Keselamatan ICT (ICTSO) bagi MPPBDR ialah Ketua Bahagian Teknologi Maklumat dari Bahagian Teknologi Maklumat MPPBDR. Peranan dan tanggungjawab ICTSO adalah: a. Membantu mengurus keseluruhan program-program keselamatan ICT MPPBDR; b. Membantu menguatkuasakan pelaksanaan Polisi Keselamatan Siber MPPBDR; c. Membantu memberi penerangan dan pendedahan berkenaan Polisi Keselamatan Siber MPPBDR kepada semua pengguna; d. Menjalankan pengurusan risiko; e. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MPPBDR berdasarkan hasil penemuan dan menyediakan laporan mengenainya; f. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;	**ICTSO**

g. Melaporkan insiden keselamatan ICT kepada Ketua Bahagian Teknologi Maklumat MPPBDR dan memaklumkannya kepada CIO; h. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; dan i. Membantu menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT. j. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
5.2.5 PENTADBIR SISTEM ICT	**PERANAN**
Pentadbir Sistem bagi MPPBDR ialah Ketua Bahagian dan PPTM di Bahagian Teknologi Maklumat. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi Keselamatan Siber MPPBDR; c. Memantau aktiviti capaian harian sistem aplikasi pengguna; d. Menjaga kerahsiaan konfigurasi sistem aplikasi dan aset ICT MPPBDR e. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; f. Menganalisis dan menyimpan rekod jejak audit; g. Menyediakan laporan mengenai aktiviti capaian secara berkala; dan h. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	**Pentadbir Sistem ICT, PPTM**

5.2.6 PENGGUNA	PERANAN
Peranan dan tanggungjawab pengguna adalah: a. Membaca, memahami dan mematuhi Polisi Keselamatan Siber MPPBDR; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Melaksanakan prinsip-prinsip Polisi Keselamatan Siber dan menjaga kerahsiaan maklumat MPPBDR; d. Melaksanakan langkah-langkah perlindungan seperti berikut :- i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menjaga kerahsiaan kata laluan; iv. Mematuhi prosedur, langkah dan garis panduan keselamatan yang ditetapkan; v. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; vi. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum dan vii. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; e. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; f. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber MPPBDR sebagaimana **Lampiran 1**.	**Semua**
5.2.7 MESYUARAT PENGURUSAN MPPBDR	**PERANAN**
Mesyuarat Pengurusan bertanggungjawab dalam keselamatan ICT. Keanggotaan adalah seperti berikut: Pengerusi : Yang Dipertua MPPBDR Ahli : Semua Ketua Jabatan / Ketua Bahagian	**Mesyuarat Pengurusan**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	47/114

Peranan : a. Memperakukan/meluluskan dokumen PKS MPPBDR; b. Memantau tahap pematuhan keselamatan ICT; c. Memperaku garis panduan, prosedur dan tatacara untuk aplikasi- aplikasi khusus dalam MPPBDR yang mematuhi keperluan PKS MPPBDR; d. Menilaiteknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; e. Memastikan PKS MPPBDR selaras dengan dasar-dasar ICT kerajaan semasa; f. Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; g. Membincang tindakan yang melibatkan pelanggaran PKS MPPBDR; dan h. Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	
2.2.8 PIHAK KETIGA	**PERANAN**
Perkara yang perlu dipatuhi oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain) bagi memastikan penggunaan maklumat dan kemudahan proses maklumat termasuk yang berikut: a. Membaca, memahami dan mematuhi Polisi Keselamatan Siber MPPBDR; b. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. Polisi Keselamatan Siber MPPBDR; ii. Tapisan Keselamatan iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. e. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber	**CIO, Ketua Bahagian ICT, ICTSO, Pentadbir Sistem ICT dan Pihak Ketiga**

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**48/114**

MPPBDR sebagaimana **Lampiran 1**.	
5.3 PENGASINGAN TUGAS *(SEGREGATION OF DUTIES)*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan c. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai production. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	
5.4 TANGGUNGJAWAB PENGURUSAN *(MANAGEMENT RESPONSIBILITIES)*	**PERANAN**
Pengurusan hendaklah memastikan warga MPPBDR, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MPPBDR supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.	**Warga MPPBDR, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MPPBDR**
5.5 HUBUNGAN DENGAN PIHAK BERKUASA *(CONTACT WITH AUTHORITIES)*	
5.5.1 PASUKAN ERT DAN CSIRT MPPBDR	**PERANAN**
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 MPPBDR; 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,	**BPTLK / BTM**

pembekal elektrik, keselamatan dan kesihatan serta bomba; dan c. Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.	
5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS *(CONTACT WITH SPECIAL INTEREST GROUPS)*	
5.6.1 WARGA MPPBDR (MENGIKUT BIDANG KEPAKARAN)	**PERANAN**
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. Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini; c. Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan d. Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	**BTM**
5.7 ANCAMAN PERISIKAN *(THREAT INTELLIGENCE)*	**PERANAN**
Teknologi Informasi dan Komunikasi (ICT) adalah serangkaian langkah dan tindakan yang diambil untuk mengesan, melindungi, dan mencegah berbagai jenis ancaman perisikan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: 1. Sistem pemantauan *(Security Monitoring)* bagi mengesan aktiviti yang mencurigakan atau ancaman perisikan yang munking terjadi di dalam rangkaian atau sistem. 2. Memasang pendinding api *(Firewall)* bagi mengawal lalu lintas jaringan rangkaian daripada aktiviti yang mencurigakan. 3. Setiap data yang disimpan hendaklah di enkripsi *(Encryption)* bagi melindungi data daripada di capai oleh orang tidak sah. 4. Memastikan setiap perisian adalah yang digunakan adalah yang terkini	**BTM**

dan sentiasa dikemaskini. 5. Mengawal akses setiap pengguna aplikasi sistem mengikut skop tugas yang telah ditetapkan oleh Bahagian Teknologi Maklumat. 6. Membahagikan rangkaian di dalam sesebuah organisasi kepada bebarapa bahagian mengikut jabatan atau sebagainya. 7. Mengkaji, menilai dan mengemaskini teknologi perkakasan atau perisian mengikut dengan keadaan semasa.	
5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK *(INFORMATION SECURITY IN PROJECT MANAGEMENT)*	
5.8.1 WARGA MPPBDR (PASUKAN PROJEK)	**PERANAN**
Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek di MPPBDR; 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 mengenai pasti kawalan-kawalan yang diperlukan; dan d. Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam Polisi Keselamatan Siber MPPBDR.	**JKJ**
5.9 MAKLUMAT INVENTORI ASET DAN YANG BERKAITAN *(INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS)*	
Untuk memberi perlindungan keselamatan yang bersesuaian ke atas semua aset ICT Majlis Perbandaran Pekan Bandar Diraja.	
5.9.1 INVENTORI ASET	**PERANAN**
Memastikan semua aset ICT MPPBDR diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut:	**Pemegang Inventori, Semua**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	51/114

a. Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini; b. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di MPPBDR; d. Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, di dokumen dan dilaksanakan; dan e. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	
5.10 MAKLUMAT PENGGUNAAN ASET YANG BOLEH DITERIMA DAN YANG BERKAITAN *(ACCEPTABLE USE OF INFORMATION AND OTHER ASSOCIATED ASSETS)*	**PERANAN**
Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.	**Warga MPPBDR**
5.11 PEMULANGAN ASET *(RETURN OF ASSETS)*	**PERANAN**
Memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak.	**Warga MPPBDR**
5.12 PENGELASAN MAKLUMAT *(CLASSIFICATION OF INFORMATION)*	**PERANAN**
Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian. Maklumat hendaklah dikelaskan dan mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan iaitu: a. **RAHSIA BESAR** - Dokumen rasmi atau maklumat rasmi yang boleh menyebabkan kerosakan yang amat besar kepada negara. *Contoh : Kertas-kertas jemaah menteri, maklumat ketenteraan.* b. **RAHSIA** - Dokumen rasmi atau maklumat rasmi yang boleh membahayakan keselamatan negara, kerosakan besar kepada kepentingan dan martabat negara atau memberi keuntungan besar kepada negara asing.	**Semua**

Contoh : Arahan penting untuk perwakilan negara yang membuat perundingan dengan negara asing. c. **SULIT** - Dokumen rasmi yang tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat negara atau kegiatan kerajaan, boleh menyebabkan kesusahan kepada pentadbiran atau orang perseorangan dan menguntungkan sebuah kuasa asing. *Contoh : Maklumat yang mungkin membolehkan pendapatan faedah kewangan daripadanya jika terdedah sebelum masa.* d. **TERHAD** - Dokumen rasmi selain daripada di atas tetapi masih perlu diberi perlindungan keselamatan. *Contoh : Perintah dan arahan biasa jabatan.*	
5.13 PELABELAN MAKLUMAT *(LABELLING OF INFORMATION)*	**PERANAN**
Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan.	**Warga MPPBDR**
5.14 PEMINDAHAN MAKLUMAT *(INFORMATION TRANSFER)*	**PERANAN**
Langkah-langkah keselamatan perlu diambil kira ketika mengendalikan maklumat seperti mengumpul, menghantar, menyimpan, memproses, menyampai, menukar dan ketika memusnah maklumat. Langkah-langkah keselamatan yang perlu diambil adalah: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menjaga kerahsiaan kata laluan; d. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; e. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; f. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui	**Semua**

umum; dan

g. Menentukan maklumat sedia untuk digunakan.

Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Perkara yang perlu dipatuhi dalam pengendalian mel elektronik dan undang-undang bertulis lain yang berkuat kuasa adalah seperti:

a. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan";
b. Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 — Pematuhan Tatacara Penggunaan E-mel dan Internet;
c. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 - Langkah-langkah mengenai penggunaan Mel Elektronik Agensi-agensi Kerajaan; dan
d. Mana-mana undang-undang bertulis Kerajaan Negeri yang berkuat kuasa;

Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut :

a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh MPPBDR sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;
b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh MPPBDR;
c. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;
d. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;
e. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak

melebihi sepuluh megabait (10Mb) atau mengikut polisi yang ditetapkan agensi semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;

f. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;

g. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

h. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;

i. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;

j. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;

k. Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera;

l. Pengguna hendaklah memastikan alamat e-mel persendirian (seperti Yahoo Mail, Gmail, Hotmail dan sebagainya) tidak digunakan untuk tujuan rasmi; dan

m. Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing.

5.15 KAWALAN AKSES (ACCESS CONTROL)	**PERANAN**

Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan Aset ICT MPPBDR.

5.15.1 KEPERLUAN KAWALAN CAPAIAN	PERANAN
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Kawalan capaian ke atas Aset ICT mengikut keperluan keselamatan dan peranan pengguna; b. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c. Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d. Kawalan ke atas kemudahan pemprosesan maklumat.	**Pentadbir Sistem ICT, Semua**
5.15.2 CAPAIAN PENGGUNA	**PERANAN**
Akaun Pengguna Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Akaun yang diperuntukkan oleh MPPBDR sahaja boleh digunakan; b. Akaun pengguna mestilah unik; c. Pemilik akaun pengguna bukanlah hak mutlak pengguna dan ia tertakluk kepada peraturan MPPBDR. Akaun boleh ditarik balik jika pengguna melanggar peraturan; d. Tidak semua pengguna boleh capai semua peringkat maklumat. Terdapat peringkat dalam capaian maklumat dengan dikawal menggunakan akaun. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; e. Penggunaan akaun milik orang lain tidak dibenarkan. f. Akaun pengguna boleh dibekukan dan ditamatkan atas sebab-sebab berikut: i. Pengguna yang bercuti panjang dalam tempoh waktu melebihi dua (2) minggu; ii. Bertukar bidang tugas kerja;	**Semua**

iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	
5.15.3 KAWALAN CAPAIAN RANGKAIAN	**PERANAN**
1. Capaian Rangkaian Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MPPBDR, rangkaian agensi lain dan rangkaian awam; b. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan c. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	**Pentadbir Sistem ICT dan ICTSO**
2. Capaian Internet Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan Internet di MPPBDR hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MPPBDR; b. Kaedah *Content Filtering* boleh digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; c. Penggunaan teknologi *(packet shaper)* untuk mengawal aktiviti *(video conferencing, video streaming, chat, downloading)* adalah perlu bagi menguruskan penggunaan jalur lebar *(bandwidth)* yang maksimum dan lebih berkesan; d. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; e. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang	**Pentadbir Rangkaian**

kerja dan terhad untuk tujuan yang dibenarkan oleh Pengarah/ pegawai yang diberi kuasa;

f. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;

g. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Bahagian sebelum dimuat naik ke Internet;

h. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;

i. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MPPBDR;

j. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan;

k. Penggunaan modem atau '*broadband*' untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan

l. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:

   i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan

   ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.

Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".

5.15.4 KAWALAN CAPAIAN SISTEM PENGOPERASIAN	
1. Capaian Sistem Pengoperasian Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan b. Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah MPPBDR menyokong perkara-perkara berikut: a. Mengesahkan pengguna yang dibenarkan; b. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf super user; dan c. Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin; b. Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; c. Mengehadkan dan mengawal penggunaan program; dan d. Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi. 2. Kad Pintar Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan;	**Pentadbir Sistem ICT dan ICTSO**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	59/114

b. Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c. Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan disyorkan untuk disekat; dan d. Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Jabatan ICT, MPPBDR.	
5.15.5 KAWALAN CAPAIAN APLIKASI DAN MAKLUMAT	**PERANAN**
Capaian Maklumat dan Sistem Aplikasi Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); c. Mengehadkan capaian sistem dan aplikasi kepada minima tiga (3) kali percubaan adalah disyorkan. Sekiranya gagal, akaun atau kata laluan pengguna boleh disekat; d. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan e. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	**Pentadbir Sistem ICT, ICTSO**
5.15.6 PERALATAN MUDAH ALIH DAN KERJA JARAK JAUH	
1. Peralatan Mudah Alih Perkara yang perlu dipatuhi adalah peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	**Semua**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	60/114

2. Kerja Jarak Jauh Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	**Semua**
5.16 PENGURUSAN IDENTITI *(IDENTITY MANAGEMENT)*	**PERANAN**
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara-perkara berikut hendaklah dipatuhi : a. Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c. Akaun pengguna yang diwujudkan pertama kali akan diberi capaian minimum yang akan ditetapkan oleh pemilik sistem; d. Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada pemilik perkhidmatan digital atau aplikasi terlebih dahulu; e. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; f. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan g. Pentadbir Sistem Aplikasi/Perkhidmatan Digital boleh membeku dan menamatkan akaun pengguna atas sebabsebab berikut : i) Pengguna bercuti panjang / menghadiri kursus di luar pejabat dalam tempoh waktu melebihi tiga (3) bulan; ii) Bertukar bidang tugas kerja; iii) Bertukar ke agensi lain; iv) Bersara; atau v) Ditamatkan perkhidmatan	**Semua Pengguna dan Warga MPPBDR**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	61/114

5.17 MAKLUMAT PENGESAHAN *(AUTHENTICATION INFORMATION)*	**PERANAN**
Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.	**ICTSO dan Pentadbir Sistem ICT**
5.17.1 PENGURUSAN KATA LALUAN	**PERANAN**
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MPPBDR seperti berikut: a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c. Panjang kata laluan ditetapkan sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus; d. Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e. Kata laluan paparan kunci (*lock screen*) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g. Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula; h. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i. Disyorkan had masa pengesahan selama lima (5) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; j. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan k. Mengelakkan penggunaan semula kata laluan yang lama digunakan.	**Semua dan Pentadbir Sistem ICT**
5.18 HAK AKSES *(ACCESS RIGHT)*	**PERANAN**
1. Satu proses untuk penyediaan akses pengguna untuk kebenaran dan	**ICTSO dan**

pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT. 2. Pemilik aset hendaklah menyemak hak akses pengguna pada sela masa yang ditetapkan. Pentadbir Perkhidmatan Aplikasi perlu mewujudkan Prosedur/SOP berkaitan Pendaftaran dan Penamatan Pengguna sistem masing- masing sebagai rujukan semakan ke atas hak akses pengguna pada sela masa yang ditetapkan. 3. Hak akses kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian atau diselaraskan apabila berlaku perubahan dalam jabatan.	**Pentadbir Perkhidmatan Aplikasi**
5.19 HUBUNGAN KESELAMATAN MAKLUMAT DENGAN PEMBEKAL *(INFORMATION SECURITY IN SUPPLIER RELATIONSHP)*	**PERANAN**
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset MPPBDR. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Mengenai pasti dan mendokumentasi jenis pembekal mengikut kategori; b. Proses kitaran hayat (*lifecycle*) yang seragam untuk menguruskan pembekal; c. Mengawal dan memantau akses pembekal; d. Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian; e. Jenis-jenis obligasi kepada pembekal; f. Pelan kontigensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat; g. Melaksanakan program kesedaran terhadap Polisi Keselamatan Siber Pejabat SUK MPPBDR kepada pembekal; h. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber MPPBDR (Lampiran 1); dan i. Pembekal perlu mematuhi arahan keselamatan yang berkuatkuasa.	**Pengurus ICT, Pemilik Projek, Pembekal**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	63/114

5.20 PERJANJIAN KESELAMATAN MAKLUMAT DENGAN PEMBEKAL *(ADDRESSING INFORMATION SECURITY WITHIN SUPPLIER AGREEMENTS)*	**PERANAN**
Perkara yang perlu dipatuhi oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain) bagi memastikan penggunaan maklumat dan kemudahan proses maklumat termasuk yang berikut: a. Membaca, memahami dan mematuhi Polisi Keselamatan Siber MPPBDR; b. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. Polisi Keselamatan Siber MPPBDR; ii. Tapisan Keselamatan iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. e. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber MPPBDR sebagaimana Lampiran 1.	**CIO, Ketua Bahagian ICT, ICTSO,** **Pentadbir Sistem ICT** **Dan Pihak Ketiga**
5.21 PENGURUSAN KESELAMATAN MAKLUMAT DALAM RANTAIAN KOMUNIKASI MAKLUMAT ICT *(MANAGING INFORMATION SECURITY IN THE INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SUPPLY CHAIN)*	**PERANAN**
Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta 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 pembekalpembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan	**Pengurus ICT, Pemilik Projek, Pembekal**

c. Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	
5.22 PEMANTAUAN, SEMAKAN DAN PERUBAHAN PENGURUSAN PERKHIDMATAN PEMBEKAL *(MONITORING, REVIEW AND CHANGE MANAGEMENT OF SUPPLIER SERVICES)*	**PERANAN**
1. MPPBDR hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. 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 dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian. 2. 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 MPPBDR 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 ICT, Pemilik Projek, Pembekal**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	65/114

5.23 KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN *AWAN (INFORMATION SECURITY FOR USE OF CLOUD SERVICES)*	PERANAN
Perkhidmatan awan adalah penting untuk memastikan bahawa organisasi memilih penyedia perkhidmatan awam yang mempunyai tahap keselamatan yang tinggi. Berikut adalah beberapa langkah-langkah yang diperlukan sebelum penggunaan perkhidmatan awan. 1. Menetapkan skop perolehan perkhidmatan awan yang ingin dikawal. Skop ini perlu merangkumi jenis perkhidmatan awan yang diperlukan, data yang akan dipindahkan ke awan, dan syarat-syarat keselamatan yang dikehendaki. 2. Melakukan penilaian risiko untuk mengenal pasti potensi ancaman dan kerentanan yang berkaitan dengan penggunaan perkhidmatan awan. Ini memungkinkan anda untuk mengenal pasti tahap risiko dan mengambil tindakan untuk mengurangkan risiko tersebut. 3. Memilih penyedia perkhidmatan awan yang mematuhi piawaian keselamatan maklumat dan memiliki rekod prestasi yang baik dalam bidang keselamatan dan privasi data. 4. Membuat perjanjian perkhidmatan dengan penyedia perkhidmatan awan yang mencakup butiran keselamatan maklumat, seperti tahap layanan, perlindungan data, pematuhan piawaian, pemisahan data, pemulihan bencana, dan peraturan pematuhan. 5. Melakukan audit keselamatan secara berkala ke atas penyedia perkhidmatan awan untuk memastikan pematuhan mereka terhadap perjanjian perkhidmatan dan piawaian keselamatan maklumat. 6. Memastikan bahawa penyedia perkhidmatan awan mempunyai perancangan pemulihan bencana yang kukuh untuk melindungi data	**ICTSO, Pentadbir Rangkaian**

organisasi dalam kejadian insiden yang merugikan. 7. Menilai semula keselamatan maklumat secara berkala dan memastikan ia selaras dengan keperluan keselamatan dan piawaian. 8. Memastikan bahawa organisasi mematuhi peraturan dan perundangan yang berkaitan dengan penggunaan perkhidmatan awan, terutamanya dalam hal privasi data dan perlindungan data peribadi.	
5.24 PERANCANGAN, PENYEDIAAN DAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY INCIDENT MANAGEMENT PLANNING AND PREPARATION)*	
Memastikan semua insiden dikendalikan dengan cepat dan berkesan serta memastikan sistem ICT MPPBDR dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej Majlis dan sistem penyampaian perkhidmatan awam.	
5.25 PENILAIAN DAN KEPUTUSAN PERISTIWA KESELAMATAN MAKLUMAT *(ASSESSMENT AND DECISION ON INFORMATION SECURITY EVENTS)*	**PERANAN**
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada MPPBDR.	**ICTSO**
5.26 MAKLUMBALAS INSIDEN KESELAMATAN MAKLUMAT *(RESPON TO INFORMATION SECURITY INCIDENT)*	**PERANAN**
Insiden keselamatan ICT bermaksud musibah *(adverse event)* yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar Polisi Keselamatan Siber sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera. Disyorkan juga insiden keselamatan ICT dilaporkan kepada pihak GCERT MAMPU:	**ICTSO, CSIRT MPPBDR**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	67/114

a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka. Prosedur pelaporan insiden keselamatan ICT berdasarkan: a. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan b. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	
5.27 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT *(LEARNING FROM INFORMATION SECURITY INCIDENTS)*	**PERANAN**
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.	**ICTSO, CSIRT MPPBDR**
5.28 PENGUMPULAN BUKTI *(COLLECTION OF EVIDENCE)*	**PERANAN**
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada MPPBDR.	**ICTSO, CSIRT MPPBDR**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	68/114

Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Tindakan menangani insiden keselamatan ICT perlu dilakukan dengan cepat, teratur dan berkesan; prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut: Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: a. Mengenal pasti jenis insiden keselamatan ICT b. Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti; c. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; d. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; e. Menyediakan tindakan pemulihan segera; dan f. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	
5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN *(INFORMATION SECURITY DURING DISRUPTION)*	**PERANAN**
1. MPPBDR hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, MPPBDR perlu mengambil kira isu- isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi MPPBDR. MPPBDR 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) MPPBDR; b. Menetapkan polisi PKP; c. Mengenai pasti perkhidmatan kritikal; d. Melaksanakan Kajian Impak Perkhidmatan *(Business Impact Analysis —*	**1. Koordinator PKP, Disaster Recovery Team (DRT), Emergency Recovery Team (ERT), Critical Communication Team (CCT) MPPBDR**

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 warga MPPBDR; g. Melaksanakan simulasi ke atas dokumen di para (c); dan h. Melaksanakan penyelenggaraan ke atas pelan di para (c).	
2. MPPBDR hendaklah menyediakan, mendokumenkan, melaksanakan dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal MPPBDR yang telah dikenal pasti berdasarkan kepada Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT terkini; b. Melaksanakan *post-mortem* dan mengemaskini pelan-pelan PKP; c. Mengemas kini pelan-pelan PKP jika berlaku perubahan kepada fungsi kritikal MPPBDR; d. Mengemas kini struktur tadbir urus PKP MPPBDR jika berlaku pertukaran pegawai bersara dan bertukar keluar; dan e. Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP.	**2. Pengurusan Tertinggi MPPBDR, Koordinator PKP, Disaster Recovery Team (DRT), Emergency Recovery Team (ERT),**
3. MPPBDR hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.	**3. Pengurusan Tertinggi MPPBDR, Koordinator PKP, Disaster Recovery Team (DRT),**

	Emergency Recovery Team (ERT), Critical Communication Team (CCT) MPPBDR, Pemilik Perkhidmatan Kritikal MPPBDR dalam PKP dan Warga MPPBDR

5.30 KETERSEDIAAN ICT UNTUK KESINAMBUNGAN *PERKHIDMATAN (ICT READINESS FOR BUSINESS CONTINUITY)*

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

5.30.1 PELAN KESINAMBUNGAN PERKHIDMATAN	**PERANAN**
Pelan Kesinambungan Perkhidmatan *(Business Continuity Management - BCM)* hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JKICT MPPBDR. Perkara-perkara berikut perlu diberi perhatian: a. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; c. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; d. Mendokumentasikan proses dan prosedur yang telah dipersetujui;	**Semua**

e. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;
f. Membuat backup; dan
g. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.

Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkaraberikut:

a. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
b. Senarai personel MPPBDR dan vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden;
c. Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;
d. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan
e. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh.

Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan.

Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. MPPBDR hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	72/114

5.31 UNDANG-UNDANG, BERKANUN, PERATURAN DAN KEPERLUAN KONTRAK *(LEGAL, STATUTORY, REGULATORY AND CONRACTUAL REQUIREMENTS)*	PERANAN
a. Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di MPPBDR: a. Arahan Keselamatan; b. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan; c. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS); d. Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan-dan-Pengendalian-Insisden-Keselamatan-Siber-Sektor-Awam e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi- Agensi Kerajaan; f. Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024; g. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009; h. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010. i. Surat Arahan Ketua Setiausaha Negara – Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006; j. Surat Arahan Ketua Pengarah MAMPU – Langkah-langkah Mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan bertarikh 1 Jun 2007 k. Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007; l. Surat Pekeliling Am Bilangan 2 Tahun 2000 – Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);	**Semua**

m. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama)- Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

n. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;

o. Akta Tandatangan Digital 1997;

p. Akta Rahsia Rasmi 1972;

q. Akta Jenayah Komputer 1997;

r. Akta Hak cipta (Pindaan) Tahun 1997;

s. Akta Komunikasi dan Multimedia 1998;

t. Perintah-Perintah Am;

u. Arahan Perbendaharaan;

v. Arahan Teknologi Maklumat 2007;

w. Akta Perlindungan Data Peribadi

x. Akta Keselamatan Siber 2024

y. Surat Pekeliling YB SUK Pahang: Bil 05 Tahun 2008: Arahan Keselamatan Penggunaan Komputer Riba Di Jabatan-jabatan Kerajaan Negeri Pahang

z. Surat Pekeliling YB SUK Pahang: Bil 08 Tahun 2009: Dasar Keselamatan ICT Pejabat SUK Negeri Pahang

aa. Surat Arahan YB SUK Pahang (13 Jan 2011): Larangan Penggunaan Perisian tidak berlesen di Komputer Milik Kerajaan

bb. Surat Arahan YB SUK Pahang (13 Jun 2011): Pendaftaran Aset Milik Persendirian dan Sumbangan

cc. Surat Arahan CIO (21 Apr 2011): Perkongsian Pencetak di Pejabat SUK Negeri Pahang dan Jabatan Negeri Pahang

dd. Surat Arahan (28 Mac 2016): Pelaksanaan Penyelenggaraan Berjadual Bagi Aset ICT Dan Peraturan Kepada Pemilik Aset ICT Pejabat Setiausaha Kerajaan Pahang

ee. Rangka Kerja Keselematan Siber Sektor Awam (RAKKSSA) V1.0 MAMPU (April 2016)

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**74/114**

5.32 HAK HARTA INTELEK *(INTELLECTUAL PROPERTY RIGHTS)*	**PERANAN**
Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	**Warga MPPBDR, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MPPBDR**
5.33 PERLINDUNGAN REKOD *(PROTECTION OF RECORDS)*	**PERANAN**
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.	**Warga MPPBDR, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MPPBDR**
5.34 PRIVASI DAN PERLINDUNGAN MAKLUMAT PENGELANAN PERIBADI (*PRIVACY AND PROTECTION OF PERSONAL IDENTIFIABLE INFORMATION (PII)*	**PERANAN**
MPPBDR hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.	**Warga MPPBDR, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MPPBDR**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	75/114

5.35 KAJIAN KEBEBASAN KESELAMATAN MAKLUMAT *(INDEPENDENT REVIEW OF INFORMATION SECURITY)*	**PERANAN**
Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat.	**Pengurus ICT dan Pemilik Perkhidmatan**
5.36 PEMATUHAN POLISI, PERATURAN DAN PIAWAIAN KESELAMATAN MAKLUMAT *(COMPLIANCE WITH POLICIES, RULES AND STANDARD FOR INFORMATION SECURITY)*	
Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Polisi Keselamatan Siber MPPBDR **1. Pematuhan Dasar** Setiap kakitangan MPPBDR perlu membaca, memahami dan mematuhi Polisi Keselamatan Siber MPPBDR dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa; Semua aset ICT di MPPBDR termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Pengarah/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT MPPBDR selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber MPPBDR. **2. Pematuhan dengan Dasar, Piawaian dan Keperluan Kawalan Teknikal Keterdedahan** Semua prosedur keselamatan dalam bidang tugas masing-masing perlu mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT. Kawalan ancaman teknikal keterdedahan perlu	**Semua**

dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi **3. Pematuhan Keperluan Audit** Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	
5.37 PROSEDUR OPERASI YANG DIDOKUMENKAN *(DOCUMENTED OPERATING PROCEDURE)*	**PERANAN**
Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan. **1. Pengendalian Prosedur** Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal; b. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	**Semua**

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**77/114**

6.0 KAWALAN MANUSIA (*PEOPLE CONTROL*)	
6.1 PEMERIKSAAN *(SCREENING)*	**PERANAN**
Menjalankan tapisan keselamatan untuk pegawai dan kakitangan MPPBDR serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan;	**Warga MPPBDR, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MPPBDR**
6.2 TERMA DAN SYARAT PEKERJAAN *(TERMS AND CONDITION EMPLOYMENT)*	**PERANAN**
Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	**Warga MPPBDR, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MPPBDR**
6.3 KESEDARAN KESELAMATAN MAKLUMAT, PENDIDIKAN DAN LATIHAN *(INFORMATION SECURITY AWARENESS AND TRAINING)*	**PERANAN**
Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MPPBDR secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa.	**Warga MPPBDR, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MPPBDR**
6.4 PROSES DISIPLIN *(DISCIPLINARY PROCESS)*	**PERANAN**
Memastikan adanya proses tindakan disiplin dan/atau undangundang ke atas pegawai dan kakitangan MPPBDR serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh MPPBDR.	**Unit Integriti**

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**78/114**

6.5 TANGGUNGJAWAB SELEPAS PENAMATAN ATAU PERUBAHAN PEKERJAAN (*RESPONSIBILITIES AFTER TERMINATION OR CHANGE OF EMPLOYMENT*)	
6.5.1 BERTUKAR ATAU TAMAT PERKHIDMATAN	**PERANAN**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan semua aset ICT dikembalikan kepada MPPBDR mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh MPPBDR dan/atau terma perkhidmatan.	**Semua**
6.6 KERAHSIAAN ATAU PERJANJIAN BUKAN PENDEDAHAN *(CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS)*	**PERANAN**
Syarat-syarat perjanjian kerahsiaan atau non-disclosure perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan. Kakitangan MPPBDR yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pembekal; b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak pembekal perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan c. Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	**ICTSO** **Pentadbir Sistem Aplikasi,** **Pengguna dan Pembekal**

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**79/114**

6.7 KERJA JAUH *(REMOTE WORKING)*	**PERANAN**
Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	**Semua**
6.8 PELAPORAN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY EVENT REPORTING)*	**PERANAN**
1. Insiden keselamatan maklumat seperti berikut hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada CERT . MPPBDR kemudiannya perlu melaporkan kepada ICTSO dengan kadar segera. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Maklumat didapati atau disyaki hilang, atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses didapati atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden- insiden yang tidak dijangka. Prosedur pelaporan insiden keselamatan Siber berdasarkan : a. Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan-dan-Pengendalian-Insisden-Keselamatan-Siber-Sektor-Awam bertarikh 1 Ogos 2022	**Warga MPPBDR, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MPPBDR**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	80/114

7.0 KAWALAN FIZIKAL *(PHYSICAL CONTROL)*	
7.1 PERIMETER KESELAMATAN FIZIKAL *(PHYSICAL SECURITY PERIMETERS)*	**PERANAN**
Kawalan fizikal kawasan adalah bertujuan untuk menghalang akses, mengesan dan mencegah cubaan menceroboh. Antara langkah-langkah keselamatan fizikal adalah; a. Lokasi hendaklah di kenal pasti dengan jelas. b. Lokasi hendaklah diprkukuhkan seperti dinding, siling, tingkap dan pintu serta dikunci untuk mengawal kemasukan; c. Memasang alat penggera atau kamera litar tertutup; d. Menghadkan jalan keluar masuk; e. Mengadakan kaunter kawalan; f. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; g. Mewujudkan perkhidmatan kawalan keselamatan. h. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; i. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan tempat-tempat yang memerlukan kawalan. j. Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; k. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan l. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	**Yang Dipertua, CIO, Pengarah Jabatan ICT, ICTSO**
7.2 KEMASUKAN FIZIKAL *(PHYSICAL ENTRY)*	**PERANAN**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Setiap kakitangan MPPBDR hendaklah memakai atau mengenakan kad pekerja sepanjang waktu bertugas; b. Setiap pelawat hendaklah mendaftar dan mendapatkan Pas Pelawat di	**Warga MPPBDR, pembekal, pakar runding dan pihak yang mempunyai urusan dengan**

Pos Pengawal dan Pas dikembalikan semula selepas tamat lawatan; c. Semua kad pekerja dan kad kuasa hendaklah diserahkan balik kepada Bahagian Sumber Manusia, Jabatan Khidmat Pengurusan apabila kakitangan berhenti atau bersara; dan d. Kehilangan kad mestilah dilaporkan dengan segera.	**perkhidmatan ICT MPPBDR**
7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN *(SECURING OFFICES, ROOMS AND FACILITIES)*	**PERANAN**
Kawasan larangan ditakrifkan sebagai kawasan yang aksesnya dihadkan kepada pegawai-pegawai yang diberi kuasa sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di MPPBDR adalah Bilik Yang Dipertua, Bilik Setiausaha, bilik-bilik Ketua Jabatan / Bahagian, Bilik Fail, Bilik Komputer dan Pusat Data. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja : Secara umumnya; a. Peralatan ICT di dalam kawasn larangan hendaklah dijaga dan dikawal supaya sentiasa dalam keadaan selamat, baik dan boleh digunakan. b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai. Semua penggunaan peralatan yang melibatkan penghantaran, pengemaskinian dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan.	**Warga MPPBDR, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MPPBDR**
7.4 PEMANTAUAN KESELAMATAN FIZIKAL *(PHYSICAL SECURITY MONITORING)*	**PERANAN**
Akses tanpa kebenaran ke kawasan fizikal terhad seperti bilik pelayan dan bilik peralatan IT boleh mengakibatkan kehilangan kerahsiaan, ketersediaan, integriti dan keselamatan aset maklumat. Berikut adalah kawalan yang boleh dilaksanakan: a) Kamera CCTV b) Pengawal keselamatan	**Warga MPPBDR, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MPPBDR**

c) Alat Penggera Penceroboh d) Alat perisian untuk pengurusan keselamatan fizikal	
7.5 PERLINDUNGAN FIZIKAL DAN ANCAMAN PERSEKITARAN *(PROTECTION AGAINST PHYSICAL AND ENVIRONMENTAL THREATS)*	**PERANAN**
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada CIO. Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; g. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan f. Akses kepada saluran riser hendaklah sentiasa dikunci.	**Pentadbir Pusat Data dan BP**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	83/114

7.6 BEKERJA DI KAWASAN YANG SELAMAT *(WORKING IN SECURE AREA)*	PERANAN
Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga MPPBDR yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis MPPBDR termasuklah Pusat Data. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas kawasan tersebut adalah seperti yang berikut: 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 MPPBDR yang telah diberi kuasa sahaja dan dipantau pada setiap masa; c. Pemantauan dibuat menggunakan *Closed-Circuit Television* (CCTV) kamera atau lain-lain peralatan yang sesuai; d. Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual; 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; j. Mengehadkan jalan keluar masuk; k. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Manual Keselamatan Dan Kesihatan Pekerja MPPBDR; dan l. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan	**Pentadbir Pusat Data dan BP**

kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut aras.	
7.7 DASAR MEJA KOSONG DAN SKRIN KOSONG *(CLEAR DESK AND CLEAR SCREEN)*	**PERANAN**
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja atau di paparan skrin apabila kakitangan tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Gunakan kemudahan password b. Log keluar apabila meninggalkan komputer; c. Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci; d. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	**Warga MPPBDR**
7.8 LOKASI DAN PERLINDUNGAN PERALATAN *(EQUIPMENT SITING AND PROTECTION)*	
Melindungi peralatan ICT MPPBDR dari kehilangan dan perkara-perkara yang boleh membahayakan.	
7.8.1 PERALATAN ICT	**PERANAN**
Dalam memastikan peralatan ICT dikawal dan dijaga dengan baik, perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Pengguna hendaklah bertanggungjawa menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; b. Pengguna hendaklah memastikan semua perkakasan disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; c. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;	**Semua**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	85/114

d. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan serta membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT;

e. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;

f. Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;

g. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

h. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT atau Juruteknik untuk di baik pulih;

i. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply (UPS);*

j. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *hub, router* dan lain-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;

k. Peralatan ICT yang hendak dibawa keluar dari premis MPPBDR, perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan;

l. Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;

m. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

n. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT;

o. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	86/114

p. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; q. Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Sistem ICT / Juruteknik; r. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; s. Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; t. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan u. Memastikan plag dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
7.9 KESELAMATAN ASET DI LUAR PREMIS *(SECURITY OF ASSETS OF PREMISES)*	**PERANAN**
Langkah-langkah yang perlu dipatuhi bagi perkakasan yang dibawa keluar dari permis MPPBDR adalah seperti dibawah; a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan; dan b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan. c. Peralatan perlu dilindungi dan dikawal sepanjang masa;	**Warga MPPBDR, Pembekal,**
7.10 MEDIA STORAN *(STORAGE MEDIA)*	**PERANAN**
Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat : a. penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;	**Semua**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	87/114

b. akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja; c. penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu dan dihapuskan dengan teratur dan selamat; d. Pergerakan media storan hendaklah direkodkan; e. Pengguna bertanggungjawab terhadap keselamatan maklumat dalam storan mudah alih seperti *thumbdrive* atau *external hard disk.* f. Perkakasan backup hendaklah diletakkan di tempat yang terkawal; g. Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan i. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
7.11 UTILITI SOKONGAN *(SUPPORTING UTILITIES)*	**PERANAN**
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti *Uninterruptable Power Supply (UPS)* dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	**Warga MPPBDR, pembekal, pakar runding dan pihak yang mempunyai urusan**
7.12 KESELAMATAN KABEL *(CABLING SECURITY)*	**PERANAN**
Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat	**Unit ICT, BP**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	88/114

hendaklah dilindungi. 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 Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui trunking bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	
7.13 PENYELENGGARAAN PERKAKASAN *(EQUIPMENT MAINTENANCE)*	**PERANAN**
Perkakasan hendaklah diselenggarakan agar tidak bermasalah bagi kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan; b. Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; d. Semua penyelenggaraan mestilah mendapat kebenaran daripada pegawai.	**Pegawai Aset, Jabatan ICT**
7.14 PELUPUSAN SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN *(SECURE DISPOSAL OR RE-USE OF EQUIPMENT)*	**PERANAN**
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MPPBDR dan ditempatkan di MPPBDR. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MPPBDR. Perkara-perkara yang perlu dipatuhi adalah	**Semua**

seperti berikut:

a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan dilakukan;
b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan;
c. Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;
d. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;
e. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;
f. Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan;
g. Pelupusan peralatan ICT hendaklah dilakukan mengikut tatacara pelupusan semasa yang berkuat kuasa.

Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:

i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya;
ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di MPPBDR;
iii. Memindah keluar dari MPPBDR mana-mana peralatan ICT yang hendak dilupuskan;
iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab MPPBDR; dan

v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti *disket* atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	91/114

8.0 KAWALAN TEKNOLOGI *(TECHNOLOGICAL CONTROL)*	
8.1 PERANTI AKHIR PENGGUNA *(USER END POINT DEVICES)*	**PERANAN**
1 Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut: a) Tamatkan sesi aktif apabila selesai tugas; 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. 2 Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek di MPPBDR; 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 mengenai pasti kawalan-kawalan yang diperlukan; dan d. Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam polisi keselamatan siber MPPBDR. Untuk tatacara lengkap penggunaan peralatan ICT rujuk kepada Tatacara dan Peraturan Infrastruktur dan Keselamatan Digital	**Warga MPPBDR, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MPPBDR**
8.2 HAK AKSES ISTIMEWA *(PRIVILEGED ACCESS RIGHT)*	**PERANAN**
Hak akses istimewa membolehkan organisasi mengawal akses kepada infrastruktur, aplikasi, aset mereka dan mengekalkan integriti semua data dan	**Pengguna, Pentadbir Perkhidmatan**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	92/114

sistem yang disimpan. Organisasi hendaklah: a. Kenal pasti senarai pengguna yang memerlukan sebarang tahap akses istimewa – sama ada untuk sistem individu – seperti pangkalan data – aplikasi atau OS asas. b. Kekalkan dasar yang memperuntukkan hak akses istimewa kepada pengguna pada apa yang dikenali sebagai "acara mengikut acara asas" - pengguna harus diberikan tahap akses berdasarkan minimum yang diperlukan untuk mereka menjalankan peranan mereka. c. Menggariskan proses kebenaran yang jelas yang berurusan dengan semua permintaan untuk akses istimewa, termasuk menyimpan rekod semua hak akses yang telah dilaksanakan. d. Pastikan hak akses tertakluk pada tarikh luput yang berkaitan. e. Ambil langkah untuk memastikan bahawa pengguna mengetahui dengan jelas sebarang tempoh masa di mana mereka beroperasi dengan akses istimewa kepada sistem. f. Jika berkaitan, pengguna diminta untuk mengesahkan semula sebelum menggunakan hak akses istimewa, untuk menjejaskan keselamatan maklumat/data yang lebih besar. g. Menjalankan audit berkala ke atas hak akses istimewa, terutamanya selepas tempoh perubahan organisasi. Hak akses pengguna harus disemak berdasarkan "tugas, peranan, tanggungjawab dan kecekapan" mereka. h. Pertimbangkan untuk beroperasi dengan prosedur yang dikenali sebagai "kaca pecah" - iaitu memastikan hak akses istimewa diberikan dalam tetingkap masa yang dikawal ketat yang memenuhi keperluan minimum untuk operasi yang akan dijalankan (perubahan kritikal, pentadbiran sistem dsb). i. Pastikan semua aktiviti akses istimewa dicatatkan dengan sewajarnya. j. Cegah penggunaan maklumat log masuk sistem generik (terutamanya nama pengguna dan kata laluan piawai). k. Mematuhi dasar memberikan pengguna dengan identiti yang	**Aplikasi, ICTSO**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	93/114

berasingan, yang membolehkan kawalan yang lebih ketat ke atas hak akses istimewa. Identiti sedemikian kemudiannya boleh dikumpulkan bersama, dengan kumpulan yang berkaitan diberikan tahap hak akses yang berbeza. l. Pastikan hak akses istimewa dikhaskan untuk tugas kritikal sahaja, yang berkaitan dengan operasi berterusan rangkaian ICT yang berfungsi – seperti pentadbiran sistem dan penyelenggaraan rangkaian.	
8.3 SEKATAN AKSES MAKLUMAT *(INFORMATION ACCESS RESTRICTION)*	**PERANAN**
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); c. Mengehadkan capaian sistem dan aplikasi kepada minima tiga (3) kali percubaan adalah disyorkan. Sekiranya gagal, akaun atau kata laluan pengguna boleh disekat; d. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan e. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	**Pengguna, Pentadbir Perkhidmatan Aplikasi, ICTSO**
8.4 AKSES KEPADA KOD SUMBER *(ACCESS TO SOURCE CODE)*	**PERANAN**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan;	**Pengarah Projek, Pengurus Projek dan Pentadbir Perkhidmatan Aplikasi**

b. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; d. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan e. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	
8.5 PENGESAHAN KESELAMATAN *(SECURE AUTHENTICATION)*	**PERANAN**
Kawalan capaian terhadap sistem aplikasi perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan adalah seperti yang berikut: a. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan; b. Menjana amaran (alert) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem; c. Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin; d. Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna; e. Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; f. Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	Pentadbir Perkhidmatan Aplikasi, ICTSO
8.6 PENGURUSAN KAPASITI *(CAPACITY MANAGEMENT)*	**PERANAN**
Perkara-perkara yang perlu dipatuhi adalah seperti 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.	**Pentadbir Sistem ICT dan ICTSO**

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**95/114**

a. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	
8.7 PERLIDUNGAN TERHADAP PERISIAN *MALWARE (PROTECTION AGAINST MALWARE)*	**PERANAN**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memasang sistem keselamatan seperti *anti virus, Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS)* untuk mengesan perisian atau program berbahaya serta mengesan aktiviti yang tidak diingini; b. Menggunakan perisian yang berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c. Mengimbas semua perisian atau sistem dengan anti virus; d. Mengemas kini pattern anti virus yang terkini; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	**Unit ICT, Pengguna**
8.8 PENGURUSAN KELEMAHAN TEKNIKAL *(MANAGEMENT OF TECHNICAL VULNERABILITIES)*	**PERANAN**
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan.	**1) Pentadbir Sistem Aplikasi dan CSIRT**

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**96/114**

Perkara yang perlu dipatuhi adalah seperti berikut: a. Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; b. Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan c. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	**MPPBDR** **2) Pengurus ICT dan Pemilik Perkhidmatan**
8.9 PENGURUSAN KONFIGURASI *(CONFIGURATION MANAGEMENT)*	**PERANAN**
Pengurusan konfigurasi ialah bahagian penting dalam operasi pengurusan aset organisasi yang lebih luas. Konfigurasi adalah kunci dalam memastikan rangkaian bukan sahaja beroperasi sebagaimana mestinya, tetapi juga dalam melindungi peranti daripada perubahan yang tidak dibenarkan atau pindaan yang salah di pihak kakitangan penyelenggaraan dan/atau vendor a. Cuba untuk menggunakan panduan khusus vendor dan/atau sumber terbuka yang tersedia secara umum tentang cara terbaik untuk mengkonfigurasi aset perkakasan dan perisian. b. Memenuhi keperluan keselamatan minimum untuk peranti, aplikasi atau sistem yang sesuai untuknya. c. Bekerja selaras dengan usaha keselamatan maklumat organisasi yang lebih luas, termasuk semua kawalan ISO yang berkaitan. d. Perlu diingat keperluan perniagaan unik organisasi - terutamanya dalam hal konfigurasi keselamatan - termasuk kebolehlaksanaan untuk menggunakan atau mengurus templat pada bila-bila masa. e. Disemak pada selang masa yang sesuai untuk memenuhi kemas kini sistem dan/atau perkakasan, atau sebarang ancaman keselamatan yang berlaku.	**ICTSO dan Pentadbir Sistem Aplikasi**
8.10 PEMADAMAN MAKLUMAT *(INFORMATION DELETION)*	**PERANAN**
Organisasi harus sedar tentang kewajipan mereka untuk memadamkan data yang disimpan pada pelayan dalaman, pemacu keras, tatasusunan dan pemacu USB apabila ia tidak lagi diperlukan dengan: a. Pilih kaedah pemadaman yang sesuai yang mematuhi mana-mana	**ICTSO dan Pentadbir Sistem Aplikasi**

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

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

8.14 KEMUDAHAN PEMPROSESAN MAKLUMAT YANG BERTINDIH *(REDUNDANCY OF INFORMATION PROCESSING FACILITIES)*	PERANAN
Kemudahan pemprosesan maklumat MPPBDR perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji *(failover test)* keberkesanannya dari semasa ke semasa.	**Pentadbir Pusat Data, Pemilik Perkhidmatan dan Pentadbir Sistem Aplikasi**
8.15 LOGGING *(LOGGING)*	**PERANAN**
1. Sistem Log Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: a. Mengadakan sistem log untuk merekod semua aktiviti harian pengguna; b. Menyemak dan meneliti sistem log untuk mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO. **2. Pemantauan Log** Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; c. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d. Aktiviti pentadbiran dan operator sistem perlu direkodkan; e. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log,	**Pentadbir Sistem ICT**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	100/114

dianalisis dan diambil tindakan sewajarnya; dan f. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MPPBDR atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	
8.16 AKTIVITI PEMANTAUAN *(MONITORING ACTIVITIES)*	**PERANAN**
Organisasi hendaklah memasukkan perkara berikut dalam operasi pemantauan mereka: a. Kedua-dua trafik rangkaian masuk dan keluar, termasuk data ke dan dari aplikasi b. Akses kepada platform kritikal organisasi, termasuk (tetapi tidak terhad kepada Sistem,Pelayan,Perkakasan rangkaian) c. Sistem pemantauan itu sendiri d. Fail konfigurasi e. Log peristiwa daripada peralatan keselamatan dan platform perisian f. Semakan kod yang memastikan mana-mana program boleh digunakan adalah dibenarkan dan bebas daripada ancaman. g. Pengiraan, penyimpanan dan penggunaan sumber rangkaian.	**ICTSO, Pentadbir Rangkaian**
8.17 PENYERAGAMAN JAM *(CLOCK SYNCHRONISATION)*	**PERANAN**
Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MPPBDR atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh Country Standard Time.	**Pentadbir Pusat Data, Pentadbir Rangkaian**
8.18 KEISTIMEWAAN PENGGUNAAN UITILITI PROGRAM *(USE OF PRIVILEGED UTILITY PROGRAMS)*	**PERANAN**
Untuk mengekalkan integriti rangkaian dan meningkatkan kesinambungan perniagaan, organisasi hendaklah: a. Hadkan penggunaan program utiliti kepada pekerja dan kakitangan	**ICTSO, Pengurus ICT, Pentadbir Rangkaian**

penyelenggaraan IT yang secara khusus memerlukan mereka menjalankan peranan kerja mereka. b. Pastikan semua program utiliti dikenal pasti, disahkan dan dibenarkan selaras dengan keperluan perniagaan, dan pihak pengurusan dapat memperoleh pandangan atas bawah penggunaannya pada bila-bila masa. c. Kenal pasti semua kakitangan yang menggunakan program utiliti, sama ada sebagai sebahagian daripada tugas harian mereka, atau secara ad-hoc. d. Laksanakan kawalan kebenaran yang mencukupi untuk mana- mana pekerja yang perlu menggunakan program utiliti, sama ada sebagai sebahagian daripada tugas harian mereka atau secara ad-hoc. e. Menghalang penggunaan program utiliti pada mana-mana sistem yang dianggap perlu oleh organisasi untuk mengasingkan tugas. f. Semak semula penggunaan program utiliti secara berkala dan sama ada alih keluar atau lumpuhkan sebarang program seperti yang diperlukan oleh organisasi. g. Program utiliti partition berbeza daripada aplikasi standard yang digunakan oleh perniagaan secara tetap, termasuk trafik rangkaian. h. Hadkan ketersediaan program utiliti, dan gunakannya untuk tujuan nyata sahaja. i. Log penggunaan program utiliti, termasuk cap masa dan pengguna yang dibenarkan.	
8.19 PEMASANGAN PERISIAN PADA SISTEM OPERASI *(INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS)*	**PERANAN**
Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan serta membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT;	**1) Pentadbir Sistem Aplikasi** **2) Pentadbir Sistem Aplikasi, Warga MPPBDR, pembekal, pakar**

	runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MPPBDR
8.20 KESELAMATAN RANGKAIAN (NETWORKS SECURITY)	**PERANAN**
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e. Firewall hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Sistem ICT; f. Semua trafik keluar dan masuk hendaklah melalui firewall di bawah kawalan MPPBDR; g. Semua perisian sniffer atau network analyser adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h. Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat MPPBDR; i. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan	**ICTSO,Pentadbir Rangkaian**

MPPBDR adalah tidak dibenarkan; k. Semua pengguna hanya dibenarkan menggunakan rangkaian MPPBDR sahaja dan penggunaan modem adalah dilarang sama sekali; dan l. Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan	
8.21 KESELAMATAN RANGKAIAN *(NETWORKS SECURITY)*	**PERANAN**
Pengurusan bagi semua perkhidmatan rangkaian *(inhouse atau outsource)* yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian.	**ICTSO, Pentadbir Sistem Aplikasi, Pembekal**
8.22 PENGASINGAN RANGKAIAN *(SEGREGATION OF NETWORKS)*	**PERANAN**
Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian MPPBDR.	**ICTSO, Pentadbir Sistem Aplikasi**
8.23 TAPISAN LAMAN WEB *(WEB FILTERING)*	**PERANAN**
Organisasi harus mewujudkan dan melaksanakan kawalan yang diperlukan untuk menghalang pekerja daripada mengakses laman web luaran yang mungkin mengandungi virus, bahan yang tidak selamat data atau jenis maklumat haram yang lain dengan: a. Laman web dengan fungsi muat naik maklumat. Akses hendaklah tertakluk kepada kebenaran dan hanya boleh diberikan atas sebab yang sah. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 atau pekeliling- peliling semasa. b. Laman web yang diketahui atau disyaki mengandungi bahan berniat jahat, seperti laman web dengan kandungan perisian yang tidak selamat. c. Pelayan perintah dan kawalan. d. Laman web berniat jahat yang diperoleh daripada scammer. e. Laman web yang mengedarkan kandungan dan bahan yang menyalahi undang-undang.	**ICTSO, Pengurus ICT, Pentadbir Rangkaian**

	POLISI KESELAMATAN SIBER	NO. DOKUMEN	PMPPBDR.PKS.01
		NO. KELUARAN	03
		NO. PINDAAN	00
		TARIKH KUATKUASA	01.06.2025
		MUKASURAT	104/114

8.24 PENGGUNAAN KRIPTOGRAFI *(USE OF CRYPTOGRAPHY)*	**PERANAN**
1. Kriptografi merangkumi kaedah-kaedah seperti yang berikut: a. Enkripsi - Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (*encryption*). b. Tandatangan Digital - Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan. 2. Pengurusan ke atas Pengurusan Infrastruktur Kunci Awam *(Public Key Infrastructure)* PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	**ICTSO, Pengurus ICT, Pentadbir Rangkain, Warga MPPBDR**
8.25 KITARAN HIDUP PEMBANGUNAN SELAMAT *(SECURE DEVELOPMENT LIFE CYCLE)*	**PERANAN**
Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Keselamatan persekitaran pembangunan; b. Keselamatan pangkalan data; c. Keperluan keselamatan dalam fasa reka bentuk; d. Keperluan check point keselamatan dalam carta perbatuan projek; e. Keperluan pengetahuan ke atas keselamatan aplikasi; f. Keselamatan dalam kawalan versi; dan g. Bagi pembangunan secara penyumberluaran (*outsource*), pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.	**ICTSO, Pentadbir Sistem Aplikasi**
8.26 KEPERLUAN KESELAMATAN PERMOHONAN *(APPLICATION SECURITY REQUIREMENTS)*	**PERANAN**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi	**Pentadbir Sistem Aplikasi, ICTSO, Pengurus ICT Pentadbir Sistem**

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**105/114**

memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; c. Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	**Aplikasi**
8.27 SENIBINA SISTEM SELAMAT DAN PRINSIP KEJURUTERAAN *(SECURE SYSTEM ARCHITECTURES AND ENGINEERING PRINCIPLES)*	**PERANAN**
Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V) sektor awam yang terkini.	**Pengurus ICT, Pentadbir Sistem Aplikasi**
8.28 PENGEKODAN SELAMAT *(SECURE CODING)*	**PERANAN**
Amalan dan prosedur pengekodan yang selamat hendaklah mengambil kira perkara berikut untuk proses pengekodan: a. Prinsip pengekodan perisian yang selamat harus disesuaikan dengan setiap bahasa pengaturcaraan dan teknik yang digunakan. b. Penggunaan teknik dan kaedah pengaturcaraan selamat seperti pembangunan yang hendak dilakukan hendaklah dibuat pengujian dan pengaturcaraan pasangan. c. Penggunaan kaedah pengaturcaraan yang berstruktur.	**Pengurus ICT,ICTSO,Pentadbir Sistem Aplikasi**

d. Dokumentasi kod yang betul dan penyingkiran kecacatan kod. e. Larangan ke atas penggunaan kaedah pengekodan perisian yang tidak selamat seperti sampel kod yang tidak diluluskan atau kata laluan berkod keras. f. Kod yang digunakan hendaklah sentiasa dikemaskini mengikut keadaan keselamatan semasa.	
8.29 UJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN *(SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE)*	**PERANAN**
1. Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut: b. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; c. Membuat semakan pengesahan di dalam aplikasi untuk mengenai pasti kesilapan maklumat; dan d. Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan. 2. Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut: Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; 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 digunapakai; dan c. Pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan *(vulnerability scanner)*.	**1) ICTSO, Pentadbir Sistem Aplikasi** **2) ICTSO, Pentadbir Sistem Aplikasi, Pengguna**

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**107/114**

8.30 PEMBANGUNAN SUMBER LUAR *(OUTSOURCED DEVELOPMENT)*	**PERANAN**
Pembangunan perisian secara outsource perlu diselia dan dipantau oleh pemilik sistem. Kod sumber *(source code)* bagi semua aplikasi dan perisian adalah menjadi hak milik MPPBDR.	**ICTSO, Pengurus ICT, Pentadbir Sistem Aplikasi**
8.31 PERSEKITARAN PEMBANGUNAN PERISIAN, PENGUJIAN DAN PENGELUARAN *(SEPARATION OF DEVELOPMENT, TEST AND PRODUCTION ENVIRONMENT)*	**PERANAN**
Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. MPPBDR 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.	**Pengurus ICT, Pentadbir Sistem Aplikasi**
8.32 PENGURUSAN PERUBAHAN *(CHANGE MANAGEMENT)*	**PERANAN**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat	**Pemilik Sistem dan Pentadbir Sistem ICT**

perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; c. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d. Akses kepada kod sumber *(source code)* aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e. Menghalang sebarang peluang untuk membocorkan maklumat.	
8.33 MAKLUMAT UJIAN *(TEST INFORMATION)*	**PERANAN**
Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; b. Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian; c. Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan d. Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar.	**ICTSO, Pentadbir Sistem Aplikasi**
8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PENGUJIAN AUDIT *(PROTECTION OF INFORMATION SYSTEMS DURING AUDIT TESTING)*	**PERANAN**
Jejak audit hendaklah mengandungi maklumat-maklumat berikut: a. Rekod setiap aktiviti transaksi; b. Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; c. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan e. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.	**ICTSO dan Pentadbir Sistem Aplikasi**

Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**110/114**

GLOSARI

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

	(*broadcast*) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi)
ICTSO	*ICT Security Officer* - Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana penggun boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian- rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan - Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapanatau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan - Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Contohnya: *Network-based* IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network* - Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	*Log-out computer* - Keluar daripada sesuatu sistem atau aplikasi komputer
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus,*trojan horse, worm, spyware* dan sebagainya.
MODEM	*Modulator DEModulator* - Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.

Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian denganbayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaranyang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yangbermotif personal dan atas sebab tertentu.
UninterruptiblePower Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

	POLISI KESELAMATAN SIBER	**NO. DOKUMEN**	**PMPPBDR.PKS.01**
		NO. KELUARAN	**03**
		NO. PINDAAN	**00**
		TARIKH KUATKUASA	**01.06.2025**
		MUKASURAT	**113/114**

LAMPIRAN 1 : AKUJANJI KESELAMATAN MAKLUMAT MPPBDR

MAJLIS PERBANDARAN PEKAN BANDAR DIRAJA

SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER MPPBDR

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

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

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

(**JAMA'IAH BINTI AHMAD**)
b.p Yang Dipertua
Majlis Perbandaran Pekan Bandar Diraja
Tarikh:

LAMPIRAN 2 : DASAR SISTEM PENGURUSAN KESELAMATAN MAKLUMAT

DASAR SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (SPKM)

Majlis Perbandaran Pekan Bandar Diraja (MPPBDR) komited untuk mengamalkan prinsip dasar SPKM dan skop keselamatan maklumat dari segi kerahsiaan, integriti dan kebolehsediaan dalam konteks organisasi bagi memastikan tadbir urus terbaik melalui penyampaian perkhidmatan yang cekap, berkesan dan berintegriti.

Sehubungan dengan itu, MPPBDR akan ;

a. Memberi jaminan dan keyakinan kepada pelanggan dan pihak berkepentingan mengenai tahap keselamatan maklumat;
b. Pematuhan kepada kehendak organisasi dan perundangan serta peraturan yang berkaitan;
c. Pembangunan objektif dan matlamat berdasarkan objektif keselamatan maklumat;
d. Memberikan komitmen bagi memenuhi keperluan berkaitan keselamatan maklumat;
e. Penilaian semula dan pengubahsuaian dasar, objektif dan sasaran untuk penambahbaikan berterusan.

Adalah menjadi tanggungjawab bagi semua kakitangan membaca, memahami dan mematuhi Dasar Sistem Pengurusan Keselamatan Maklumat (SPKM) Majlis Perbandaran Pekan Bandar Diraja. Tindakan tatatertib boleh diambil ke atas kakitangan bagi sebarang ketakakuran dan pelanggaran dasar ini.

YANG DIPERTUA
MAJLIS PERBANDARAN PEKAN BANDAR DIRAJA
1 JUN 2025

No. Rujukan : MPPBDR/BTM/P/01
No. Pindaan/Keluaran : 02/03