

**POLISI
UNIT
TEKNOLOGI
MAKLUMAT**

HOSPITAL PENDANG





HOSPITAL PENDANG KEDAH DARUL AMAN

POLISI DAN PROSEDUR

JABATAN/UNIT: UNIT TEKNOLOGI MAKLUMAT, BAHAGIAN PENGURUSAN

NO DOKUMEN	BILANGAN 1
NO KELUARAN	01/2023
NO PINDAAN	

DISEDIAKAN	JAWATAN	TARIKH
SHUHAIZA ASZRIN BINTI MOHD KASIM NAMA & TANDATANGAN DISEMAK	KETUA UNIT TEKNOLOGI MAKLUMAT	
SALMI BINTI SALIM NAMA & TANDATANGAN DILULUSKAN	TIMBALAN PENGARAH PENGURUSAN	
MEJAR BERSEKUTU (PA) DR. MUHAMMAD SHAUQI BIN HAJI ABDUL KADIR	PENGARAH HOSPITAL PENDANG	

AKRONIM	4
ISTILAH DAN DEFINISI	4
A. ORGANISASI DAN PENGURUSAN	6
1. PENGENALAN.....	6
2. TUJUAN.....	6
3. LATARBELAKANG	7
4. VISI	8
5. MISI.....	8
6. OBJEKTIF	8
7. PIAGAM PELANGGAN.....	8
8. SKOP PERKHIDMATAN	10
9. STRUKTUR ORGANISASI UNIT	11
B. SUMBER MANUSIA	12
1. KETUA UNIT	12
2. PEGAWAI KESELAMATAN ICT (ICTSO)	12
3. PENTADBIR SISTEM APLIKASI	13
4. PENTADBIR RANGKAIAN	13
5. PENTADBIR BILIK SERVER	14
6. PENGGUNA.....	14
C. PERALATAN DAN KEMUDAHAN	15
1. PRINSIP ASAS	15
2. PERKAKASAN DAN PERISIAN ICT.....	15
D. PROSEDUR DAN TATACARA	17
1. TATACARA PENGGUNAAN PERKAKASAN ICT	17
2. PENGURUSAN DAN PENYELENGGARAAN PERKAKASAN ICT	18
3. TATACARA PEMINJAMAN PERKAKASAN DAN PERISIAN ICT	19
4. TATACARA PENGURUSAN DAN PENGGUNAAN EMEL	21
5. TATACARA PENGGUNAAN INTERNET	22
6. TATACARA PENGGUNAAN DAN PENGURUSAN RANGKAIAN	24
7. PENGGUNAAN DAN PENGURUSAN SISTEM APLIKASI	25
8. PENGURUSAN BILIK SERVER	26
9. PEMBANGUNAN DAN PENGURUSAN LAMAN WEB.....	27
PEMAKAIAN	29
PENGECUALIAN	29
TARIKH KUATKUASA	29

AKRONIM

ICT	Teknologi Maklumat dan Komunikasi
ICTSO	Pegawai Keselamatan ICT
KKM	Kementerian Kesihatan Malaysia
MAMPU	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
JPICT	Jawatankuasa Pemandu ICT
JPA	Jabatan Perkhidmatan Awam
DKICT	Dasar Keselamatan ICT
CERT	Pasukan Tindak Balas Insiden Keselamatan ICT

ISTILAH DAN DEFINISI

ISTILAH	DEFINISI
Perisian	Program atau atur cara komputer yang dapat digunakan dengan sistem komputer tertentu. Perisian boleh terdiri daripada perisian sistem atau perisian aplikasi. Perisian adalah produk yang tersedia di pasaran untuk kegunaan pengguna komputer berdasarkan keperluan umum. Contoh perisian adalah seperti sistem operasi <i>Windows, Adobe, Microsoft Office</i> dan <i>AutoCAD</i> .
Sistem Aplikasi	Perisian yang direkabentuk dan dibangunkan khas untuk kegunaan pengguna komputer yang khusus dan spesifik sama ada yang dibangunkan secara dalaman atau menggunakan perkhidmatan syarikat pembangunan sistem. Contoh sistem aplikasi adalah Sistem Kewangan dan Perakaunan.
Perkakasan ICT	Komponen fizikal yang dihubungkan secara terus dengan komputer atau sistem yang lain. Ia juga merupakan alat yang digunakan sebagai input, dan aktiviti pemprosesan serta output.
<i>Firewall</i>	Peralatan atau perisian yang berfungsi untuk mengawal capaian internet dan melindungi sesebuah rangkaian komputer daripada serangan-serangan dan pencerobohan oleh pihak luar yang tidak bertanggung jawab.

ISTILAH	DEFINISI
<i>Switches</i>	Peralatan yang menghubungkan beberapa segmen rangkaian komputer di dalam rangkaian setempat (<i>Local Area Network</i>).
<i>Server</i>	Komputer berkapasiti tinggi yang menyediakan pelbagai jenis perkhidmatan untuk diakses oleh lain-lain komputer yang berhubung di dalam rangkaian.
<i>Wireless Access Point</i> atau <i>WiFi</i>	Peralatan yang membenarkan peralatan tanpa wayar untuk dihubungkan ke rangkaian dengan menggunakan piawaian rangkaian tanpa wayar.
<i>Local Area Network (LAN)</i>	Rangkaian Kawasan Setempat (<i>Local Area Network</i>) yang menghubungkan peranti dalam satu pejabat atau satu bangunan.
<i>Wide Area Network (WAN)</i>	Rangkaian Kawasan Luas (<i>Wide Area Network</i>). Pengguna boleh menghantar data, audio dan video pada jarak yang jauh sehingga merangkumi sebuah negara atau benua atau seluruh dunia.
<i>PC</i>	Komputer Peribadi
Perkakasan rangkaian	Perkakasan dan komponen yang digunakan dalam sistem rangkaian seperti switch, hub, router dan sebagainya
IP	<i>Internet Protocol</i>
Pengguna	Seseorang sama ada Pegawai, Pembekal, Pakar Runding atau Pelawat yang dibenarkan menggunakan kemudahan ICT Hospital Pendang
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.

A. ORGANISASI DAN PENGURUSAN

1. PENGENALAN

1.1 Polisi Unit Teknologi Maklumat, Hospital Pandang mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi semasa menggunakan infrastruktur teknologi maklumat dan komunikasi (ICT). Polisi juga menerangkan tanggungjawab pengguna dalam melindungi kemudahan ICT yang disediakan di Hospital Pandang.

1.2 Polisi ini perlu dibaca bersama dengan dokumen – dokumen berikut:

- a. Pelan Strategik Pendigitalan Kementerian Kesihatan Malaysia 2021-2025
- b. Surat Pekeliling Ketua Setiausaha Kementerian Kesihatan Malaysia Bilangan 10 Tahun 2019: Dasar Keselamatan ICT Versi 5.0 Kementerian Kesihatan Malaysia
- c. Surat Pekeliling AM Kementerian Kesihatan Bilangan 1 Tahun 2016: Tatacara Pelaksanaan Projek ICT di Kementerian Kesihatan Malaysia.
- d. Surat Pekeliling AM Kementerian Kesihatan Bilangan 2 Tahun 2016: Garis Panduan Kesediaan Infrastruktur Teknologi Maklumat dan Komunikasi (ICT) di Agensi dan Fasilitas Kementerian Kesihatan Malaysia
- e. Garis Panduan Pelaksanaan Sidang Video di Kementerian Kesihatan Malaysia
- f. Tata Etika Penggunaan Media Sosial oleh Warga KKM
- g. Garis Panduan Pengendalian Insiden Keselamatan ICT KKM
- h. Surat Pekeliling Ketua Setiausaha Kementerian Kesihatan Malaysia Bilangan 2 Tahun 2023: Garis Panduan Pelaksanaan Rasionalisasi Pencetak di Kementerian Kesihatan Malaysia
- i. Garis Panduan Portal MyGovernment dan Laman Web/ Portal Agensi-Agensi Sektor Awam

2. TUJUAN

2.1. Polisi Unit Teknologi Maklumat, Hospital Pandang ini disediakan bagi tujuan menambah baik tadbir urus Unit Teknologi Maklumat dalam meningkatkan kualiti perkhidmatan dan pengoperasian ICT kepada warga kerja Hospital Pandang.

2.2. Tujuan polisi ini adalah seperti berikut:

- a. Mewujudkan polisi ICT yang sentiasa relevan dengan persekitaran perkhidmatan kesihatan.

- b. Memastikan infrastruktur ICT dan rangkaian menyokong adaptasi teknologi baharu dan dikawal selia dengan baik.
- c. Memastikan isu-isu kerahsiaan, keselamatan, bidang kuasa dan etika pengguna ICT dilindungi dan diuruskan melalui saluran yang betul.
- d. Menyediakan rangka-kerja dan sumber rujukan yang lengkap mengenai hal ehwal Teknologi Maklumat.
- e. Mendukung usaha pendigitalan perkhidmatan kerajaan dengan memastikan penggunaan sistem aplikasi secara cloud dan sistem aplikasi sokongan yang disediakan oleh KKM, MAMPU, JPA dan Kementerian Kewangan.

3. LATARBELAKANG

Unit Teknologi Maklumat adalah salah satu unit di bawah Bahagian Pengurusan. Unit ini menyediakan perkhidmatan sokongan teknikal infrastruktur ICT dan bertanggungjawab menyebarkan sumber informasi dan perkembangan teknologi baharu ICT yang dapat memberi sumbangan ke arah kecekapan pentadbiran hospital.

Pada awalnya di penghujung tahun 2022, dua orang pegawai FA32 (KUP) telah dilantik secara pentadbiran yang mana dipertanggungjawabkan untuk menguruskan sistem rangkaian dan sistem dalaman. Dengan lantikan ini, Unit Teknologi Maklumat mula beroperasi seawal bulan oktober, 2022 sehinggalah perjawatan baru diluluskan oleh MAMPU pada Mac 2023. Selepas perjawatan diluluskan, tiga (3) lagi jawatan telah di isi secara berperingkat sehingga Jun 2023.

Dari aspek pengembangan perkhidmatan, Unit Teknologi Maklumat telah melaksanakan perkhidmatan berikut sejajar dengan pengisian perjawatan;

- a. Meluaskan perkhidmatan rangkaian WiFi dimana dahulunya hanya boleh diakses untuk kakitangan, sekarang juga boleh diakses untuk peralatan perubatan dan orang awam.
- b. Mengurus, memantau dan mengendalikan perkakasan ICT yang telah dipasang pada 1 Ogos 2022 tanpa bantuan syarikat / kontraktor.
- c. Membangun laman web rasmi Hospital Pendang bermula Julai 2023.
- d. Membantu secara teknikal dalam memberi khidmat sokongan teknikal terhadap penggunaan sistem aplikasi KKM dan sistem aplikasi sokongan yang diputuskan untuk digunakan di hospital.
- e. Memberi latihan penggunaan sistem aplikasi dan terlibat secara langsung dalam program orientasi kakitangan baharu.

- f. Memberi bantuan teknikal bagi penggunaan bilik mesyuarat, bilik perbincangan dan bilik latihan ICT (jika perlu).
- g. Berusaha melaksanakan dan memberi perkhidmatan yang cekap mengikut piagam pelanggan.

4. VISI

Ke arah memodenkan pentadbiran Hospital Pendang dengan teknologi ICT yang terkini dan melahirkan warga hospital yang membudayakan serta mengaplikasikan ICT bagi memberi perkhidmatan yang berkualiti, cekap dan mesra ICT.

5. MISI

Menyediakan kemudahan infrastruktur dan infostruktur yang berkualiti bagi menyokong perkhidmatan sokongan kepada pentadbiran Hospital Pendang seiring dengan perkembangan teknologi ICT terkini bagi menjamin sistem perkhidmatan dapat dilaksanakan secara optimum.

6. OBJEKTIF

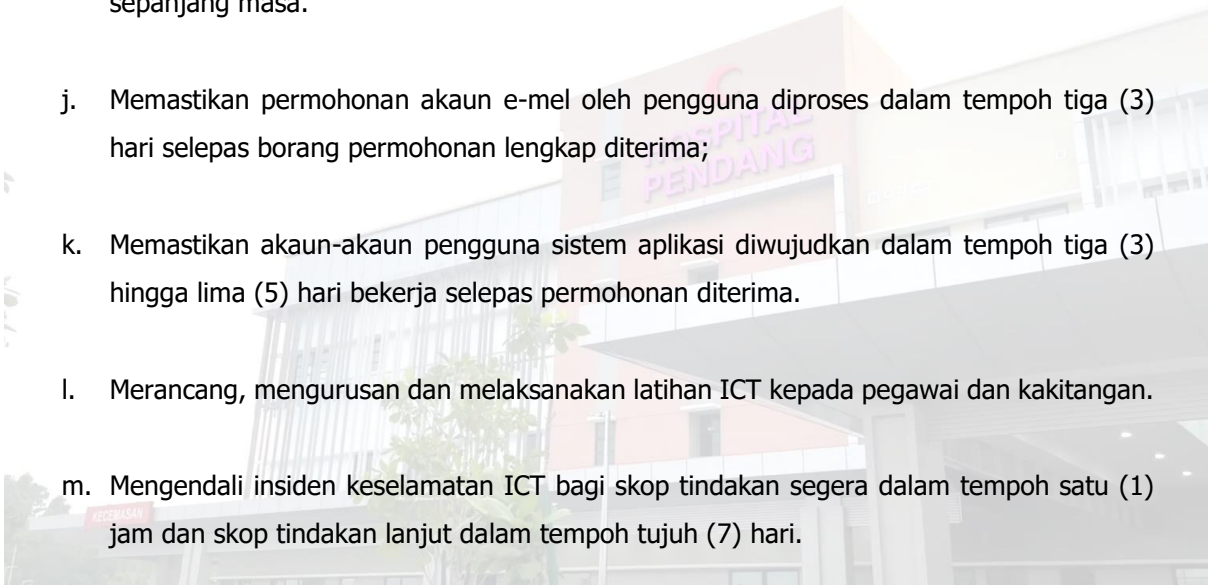
Menawarkan perkhidmatan ICT yang efisien kepada semua jabatan dan unit di Hospital Pendang bagi meningkatkan kualiti operasi harian selain meluaskan penggunaan ict dikalangan warga kerja hospital.

7. PIAGAM PELANGGAN

Unit Teknologi Maklumat, Hospital Pendang adalah komited dan penuh tekad berikrar akan menumpukan seluruh tenaga dan usaha kami untuk:

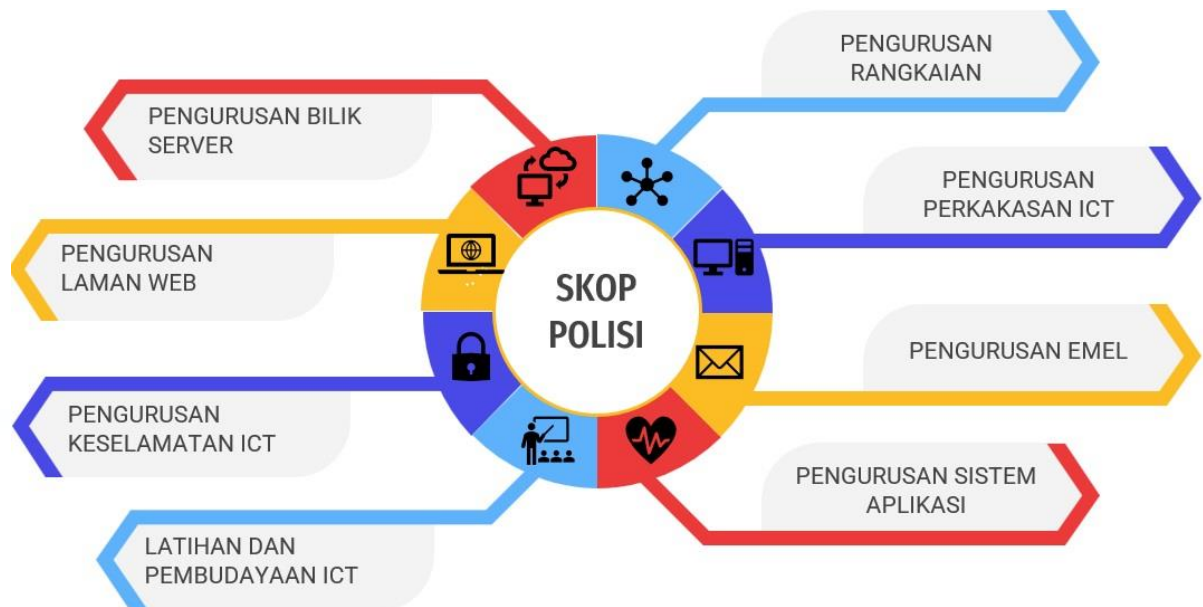
- a. Memberi perkhidmatan sokongan teknikal ICT (Helpdesk) melalui bantuan telefon dalam tempoh dua (2) jam dan bantuan secara *on-site* (tidak melibatkan penggantian perkakasan) dalam tempoh dua (2) hari bekerja;
- b. Memastikan semua aduan kerosakan perkakasan ICT yang diterima diberi maklum balas awal dalam tempoh dua (2) jam;
- c. Menyelesaikan kerosakan perkakasan ICT yang tidak melibatkan penggantian alat ganti dalam tempoh tiga (3) hari bekerja;
- d. Memberi keputusan permohonan pinjaman perkakasan ICT dalam tempoh satu (1) hari bekerja dari tarikh permohonan lengkap diterima;

- e. Melaksana penyelenggaraan perkakasan ICT (tanpa melibatkan syarikat atau kontraktor) sekurang - kurangnya sekali (1) dalam setahun;
- f. Merancang, menyelaraskan dan melaksanakan perolehan dan pembekalan perkakasan, perisian dan kemudahan infrastruktur ICT mengikut keperluan;
- g. Merancang, mengurus dan menyelenggara rangkaian, peralatan rangkaian dan bilik server mengikut keperluan;
- h. Memastikan gangguan teknikal rangkaian yang tidak melibatkan fizikal dipulihkan dalam tempoh dua puluh empat (24) jam, melibatkan kerosakan fizikal dalam tempoh empat puluh lapan (48) jam;
- i. Memastikan laman web rasmi Hospital Pendang sentiasa dikemaskini dan boleh dicapai sepanjang masa.
- j. Memastikan permohonan akaun e-mel oleh pengguna diproses dalam tempoh tiga (3) hari selepas borang permohonan lengkap diterima;
- k. Memastikan akaun-akaun pengguna sistem aplikasi diwujudkan dalam tempoh tiga (3) hingga lima (5) hari bekerja selepas permohonan diterima.
- l. Merancang, mengurus dan melaksanakan latihan ICT kepada pegawai dan kakitangan.
- m. Mengendalikan insiden keselamatan ICT bagi skop tindakan segera dalam tempoh satu (1) jam dan skop tindakan lanjut dalam tempoh tujuh (7) hari.



8. SKOP PERKHIDMATAN

8.1 Polisi ini merangkumi skop perkhidmatan seperti berikut:



8.2 Skop polisi Pengurusan Rangkaian meliputi perkhidmatan rangkaian MyGovNet, pengurusan penggunaan WiFi, pengendalian infrastruktur keselamatan rangkaian dan pengendalian infrastruktur rangkaian.

8.3 Skop polisi Pengurusan Perkakasan ICT meliputi perkhidmatan perolehan perkakasan ICT dan rangkaian, pengurusan sewaan perkakasan ICT, pengurusan penyelenggaraan perkakasan ICT dan khidmat sokongan teknikal.

8.4 Skop polisi Pengurusan Sistem Aplikasi meliputi penggunaan dan pengurusan sistem aplikasi KKM, sistem aplikasi kewangan dan sistem aplikasi digital kerajaan.

8.5 Skop polisi Pengurusan Bilik Server hanya mencakupi pemantauan dan pengurusan peralatan rangkaian dan peralatan keselamatan rangkaian termasuk rak dan kabel yang terdapat di dalamnya.

8.6 Skop polis Pengurusan Laman Web adalah termasuk dari peringkat pembangunan Laman Web, pengujian, susun atur kandungan dan memastikan kandungan sentiasa dikemaskini.

8.7 Skop Pengurusan Keselamatan ICT di KKM hanya melibatkan pendaftaran dan pengisian sistem ePatuh serta pengurusan pengendalian insiden ICT.

9. STRUKTUR ORGANISASI UNIT



Berikut adalah maklumat perjawatan dan sumber sedia ada:

Bil	Jawatan	Jumlah
1.	Pegawai Teknologi Maklumat F41/F44	1
2.	Penolong Pegawai Teknologi Maklumat F29/F32	2
3.	Juruteknik FT19/FT22	1

B. SUMBER MANUSIA

1. KETUA UNIT

Skop fungsi bidang tugas dan tanggungjawab Ketua Unit Teknologi Maklumat secara umumnya adalah seperti berikut:

- a. Tertakluk kepada Terma Rujukan Ketua Unit Hospital merujuk surat HOPE.500-4/2/2 (26) bertarikh 14 September 2023.
- b. Memimpin dalam pelaksanaan projek ICT seiring dengan misi, visi dan objektif hospital.
- c. Merangka, merumus dan menguatkuasa Polisi Unit Teknologi Maklumat.
- d. Bertanggungjawab menyelaras perancangan ICT serta melaksana, mengawal dan menilai dasar pengurusan maklumat hospital.
- e. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan hospital.
- f. Menjalankan kerja-kerja pengurusan insiden keselamatan ICT dan kerja-kerja audit keselamatan ICT.
- g. Merancang dan melaksanakan urusan perolehan perkakasan, perisian dan lain-lain keperluan ICT.
- h. Mengurus, memantau dan melaksanakan pengurusan dan penyelenggaraan rangkaian.
- i. Menentukan kawalan akses semua pengguna terhadap Aset ICT di Hospital Pendang.

2. PEGAWAI KESELAMATAN ICT (ICTSO)

Peranan dan tanggungjawab ICTSO Hospital Pendang yang dilantik oleh *National Cyber Coordination And Command Centre (NC4)* adalah seperti berikut:

- a. Melaksanakan kawalan keselamatan ICT selaras dengan keperluan KKM;
- b. Memberi penerangan dan pendedahan berkenaan DKICT KKM kepada semua pengguna;
- c. Menjalankan pengurusan risiko;
- d. Menjalankan audit dalaman, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya;
- e. Melaporkan insiden keselamatan ICT kepada CERT KKM;
- f. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;
- g. Memantau pematuhan DKICT KKM;
- h. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; dan
- i. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan dan pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baharu dapat dielakkan.

3. PENTADBIR SISTEM APLIKASI

Peranan dan tanggungjawab Pentadbir Sistem ICT dari aspek keselamatan ICT adalah seperti berikut:

- a. Memastikan kerahsiaan kata laluan aset ICT;
- b. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;
- c. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT KKM;
- d. Memantau aktiviti capaian harian sistem aplikasi pengguna;
- e. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikanannya dengan serta merta;
- f. Menyimpan dan menganalisis rekod audit trail;
- b. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala;
- c. Bertanggungjawab memantau setiap peralatan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; dan
- d. Bertanggungjawab memastikan setiap perolehan perisian ICT adalah tulen.

4. PENTADBIR RANGKAIAN

Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut:

- a. Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di Hospital Pengang beroperasi sepanjang masa;
- b. Memastikan semua perkakasan dan perisian rangkaian diselenggara dengan sempurna;
- c. Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada;
- d. Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil;
- e. Melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT (*Security Posture Assessment, SPA*) serta penilaian risiko keselamatan maklumat;
- f. Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian hospital secara tidak sah seperti peralatan *modem, wireless access points, broadband* dan *dial-up*;
- g. Menyediakan zon khas rangkaian untuk tujuan pengujian perkakasan dan perisian rangkaian; dan
- h. Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian.

5. PENTADBIR BILIK SERVER

Pentadbir bilik server adalah bertanggungjawab kepada perkara-perkara berikut:

- a. Mengawal dan mengurus setiap aktiviti yang berlaku di dalam bilik server dan memastikan bilik server bebas daripada aktiviti sabotaj, kecurian dan jenayah melalui sistem pemantauan yang berterusan;
- b. Memantau dan merekod maklumat personel yang keluar dan masuk ke bilik server melalui sistem akses dan Merekodkan semua pergerakan keluar/masuk Bilik Server dalam Buku Daftar Rekod;
- c. Melaksanakan kawalan akses melalui konsep "Siapa anda dan kenapa anda di sini?";
- d. Personel agensi dan jika perlu, kontraktor dan pengguna hendaklah diberikan latihan, program kesedaran serta dikemaskinikan dengan dasar dan prosedur agensi yang berkaitan dengan tugas mereka secara berkala; dan
- e. Sentiasa menjaga kebersihan dan kekemasan Bilik Server supaya tidak terdedah kepada habuk dan memastikan tidak menyimpan atau menempatkan peralatan yang tidak diperlukan.

6. PENGGUNA

Peranan dan tanggungjawab Pengguna adalah seperti berikut:

- a. Membaca, memahami dan mematuhi Polisi ICT Hospital Pendang;
- b. Melaksanakan prinsip-prinsip Polisi ICT Hospital Pendang dan menjaga kerahsiaan maklumat Hospital Pendang;
- c. Melaksanakan langkah-langkah perlindungan seperti berikut:
 - i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
 - ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
 - iii. Menentukan maklumat sedia untuk digunakan;
 - iv. Menjaga kerahsiaan kata laluan;
 - v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
 - vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
 - vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.
- d. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; dan
- e. Menghadiri program dan latihan mengenai ICT.

C. PERALATAN DAN KEMUDAHAN

1. PRINSIP ASAS

Polisi ICT Hospital Pandang menetapkan prinsip asas seperti berikut:

- a. Pengurusan Tertinggi diperuntukkan sebuah komputer peribadi atau komputer bimbit dan sebuah pencetak.
- b. Ketua Jabatan, Pengurus dan Ketua Unit diperuntukkan sebuah komputer dan sebuah pencetak.
- c. Semua kakitangan dari kumpulan Pengurusan dan Profesional yang bertaraf tetap/kontrak diperuntukkan sebuah komputer.
- b. Semua bahagian dan unit dilengkapi dengan komputer yang mencukupi dan satu unit laptop bagi kegunaan rasmi bahagian dan unit masing-masing.
- c. Pelaksanaan rasionalisasi pencetak selaras dengan pekeliling sedia ada Surat Pekeliling Ketua Setiausaha Kementerian Kesihatan Malaysia Bilangan 2 Tahun 2023: Garis Panduan Pelaksanaan Rasionalisasi Pencetak di Kementerian Kesihatan Malaysia.
- d. Penggunaan mesin fotokopi hendaklah dipusatkan di setiap bahagian dan unit bagi kegunaan guna sama.

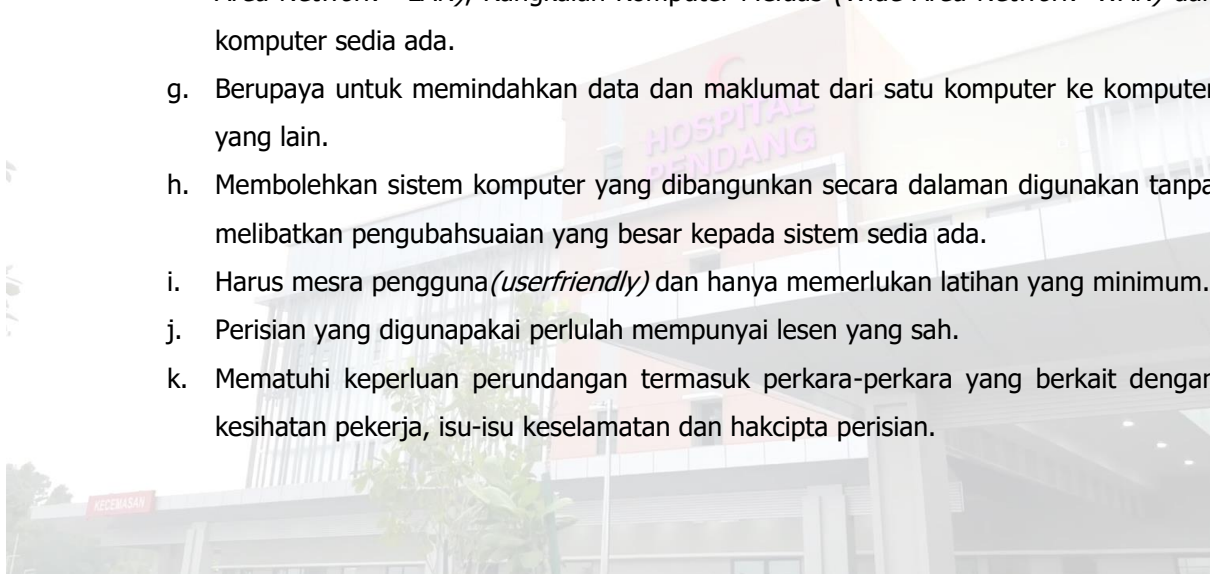
2. PERKAKASAN DAN PERISIAN ICT

- 2.1. Proses perolehan Perkakasan dan Perisian ICT hendaklah merujuk kepada pekeliling terpakai sedia ada iaitu Surat Pekeliling AM Kementerian Kesihatan Bilangan 1 Tahun 2016: Tatacara Pelaksanaan Projek ICT di Kementerian Kesihatan Malaysia.
- 2.2. Perincian norma pengagihan Perkakasan ICT hendaklah merujuk kepada pekeliling terpakai sedia ada iaitu Surat Pekeliling AM Kementerian Kesihatan Bilangan 2 Tahun 2016: Garis Panduan Kesediaan Infrastruktur Teknologi Maklumat dan Komunikasi (ICT) di Agensi dan Fasiliti Kementerian Kesihatan Malaysia
- 2.3. Norma kerja yang sesuai untuk dipertimbangkan dalam pengagihan laptop adalah salah satu seperti berikut:
 - a. Menjalankan kajian mengikut bidang kerja dan penyediaan kertas kerja serta laporan yang berkaitan;
 - b. Sering menjalankan tugas-tugas rasmi di luar pejabat yang memerlukan penggunaan laptop;
 - c. Sering memberi taklimat yang berkaitan dengan bidang kerja serta kajian berkenaan; dan

- d. Menjalankan tugas berkaitan dengan pembangunan dan pengurusan aplikasi serta pengurusan keselamatan dan operasi ICT.

2.4. Kemudahan perkakasan dan perisian ICT yang disediakan hendaklah dipastikan mempunyai ciri-ciri berikut:

- a. Setiap komputer dilengkapi dengan perisian asas seperti sistem pengoperasian, system automasi pejabat, pelayar web, anti-virus dan perisian *remote* akses untuk tujuan pentadbiran dan penyelenggaraan.
- b. Dewan Persidangan, Bilik Seminar dan semua bilik CME di jabatan dan wad disediakan dengan kemudahan komputer dan capaian internet.
- c. Bilik Mesyuarat Utama disediakan kemudahan sidang video (*Video Conferencing*) berdasarkan keperluan.
- d. Sistem komputer beroperasi 24 jam sehari dengan kadar *downtime* yang minimum.
- e. Mengambil kira teknologi dan versi terkini serta mampu dipertingkatkan.
- f. Mempunyai keterkaitan (*connectivity*) dengan Rangkaian Komputer Setempat (*Local Area Network - LAN*), Rangkaian Komputer Meluas (*Wide Area Network - WAN*) dan komputer sedia ada.
- g. Berupaya untuk memindahkan data dan maklumat dari satu komputer ke komputer yang lain.
- h. Membolehkan sistem komputer yang dibangunkan secara dalaman digunakan tanpa melibatkan pengubahsuaian yang besar kepada sistem sedia ada.
- i. Harus mesra pengguna (*userfriendly*) dan hanya memerlukan latihan yang minimum.
- j. Perisian yang digunakan perlulah mempunyai lesen yang sah.
- k. Mematuhi keperluan perundangan termasuk perkara-perkara yang berkait dengan kesihatan pekerja, isu-isu keselamatan dan hakcipta perisian.



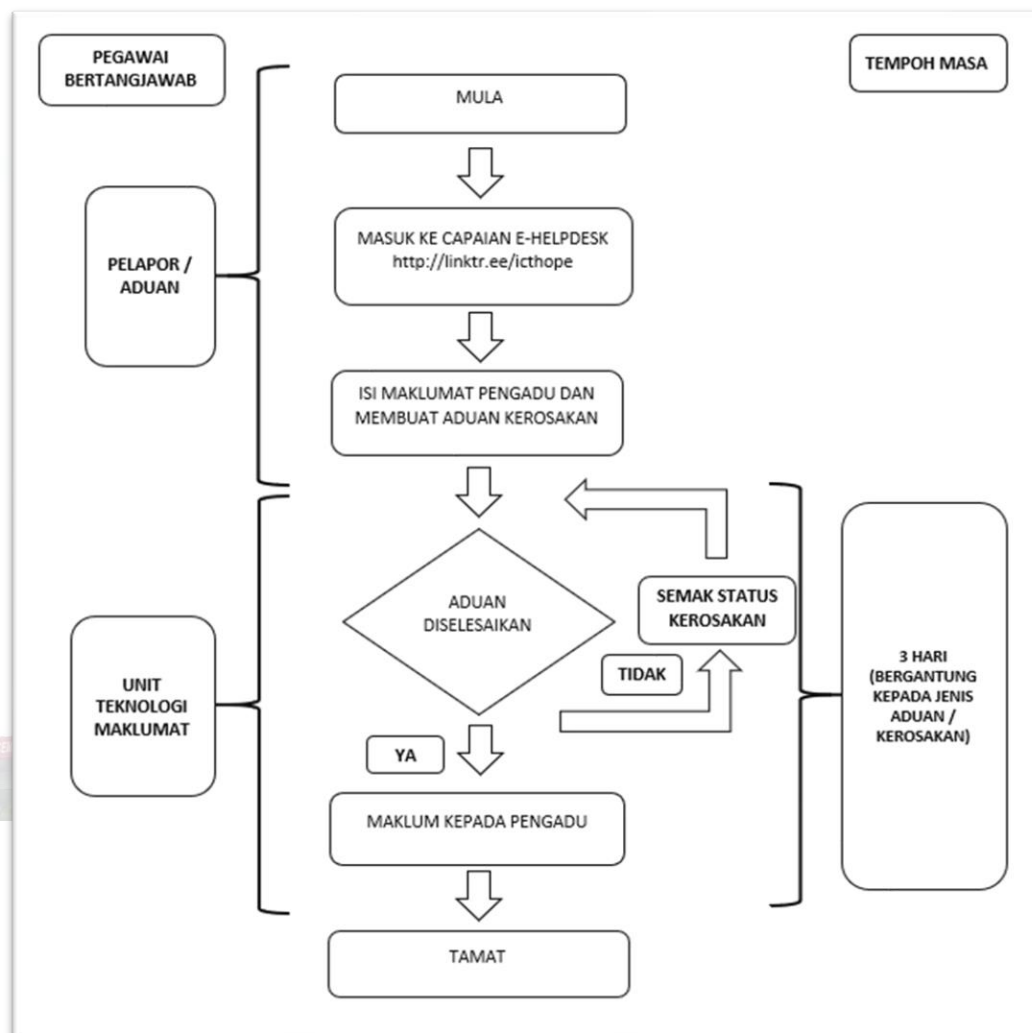
D. PROSEDUR DAN TATACARA

1. TATACARA PENGGUNAAN PERKAKASAN ICT

- 1.1. Semua perkakasan ICT yang telah dibekalkan adalah hakmilik Hospital Pendang dan hendaklah digunakan untuk urusan pejabat sahaja.
- 1.2. Adalah menjadi tanggungjawab pegawai dan kakitangan yang telah dibekalkan perkakasan ICT untuk:
 - a. memastikan perkakasan ICT disimpan dengan selamat;
 - b. digunakan dengan baik mengikut peraturan norma penggunaan perkakasan; dan
 - c. melaporkan kepada Unit Pengurusan Aset sekiranya berlaku kehilangan perkakasan ICT; dan sekiranya terdapat kerosakan perkakasan ICT hendaklah dilaporkan terus ke Unit Teknologi Maklumat.
- 1.3. Perkakasan ICT seperti set komputer, pencetak yang dibekalkan tidak dibenarkan dipindah dari lokasi asal yang telah ditetapkan tanpa kelulusan Pegawai Aset Hospital Pendang.
- 1.4. Bagi perkakasan ICT yang digunakannya dalam sesebuah unit/bahagian, pengurusan unit/bahagian tersebut perlu mewujudkan satu sistem pemantauan penggunaan perkakasan ICT seperti Buku Pergerakan Perkakasan ICT.
- 1.5. Pengguna tidak dibenarkan memasang mana-mana perisian/program ke dalam komputer/komputer bimbit yang dibekalkan. Sebarang pemasangan perisian/program yang diperlukan akan dilakukan oleh Unit Teknologi Maklumat.
- 1.6. Bagi penggunaan *thumbdrive*, adalah menjadi tanggungjawab pengguna untuk memastikan data-data dalam *thumbdrive* dibuat penduaan seperti di dalam *hard disk* atau media storan yang lain. Ini adalah kerana *thumbdrive* yang dibekalkan merupakan media storan sementara dan juga kadang kala media tersebut mudah rosak, menyebabkan kehilangan data-data yang disimpan dalamnya.
- 1.7. Sekiranya berlaku kerosakan atau kehilangan perkakasan ICT, pengguna yang bertanggungjawab melalui Ketua Jabatan / Ketua Unit adalah dikehendaki membuat laporan rasmi atau laporan polis berdasarkan jenis dan kos perkakasan. Semua laporan perlu dikemukakan kepada Pegawai Aset Hospital Pendang.

2. PENGURUSAN DAN PENYELENGGARAAN PERKAKASAN ICT

- 2.1. Unit Teknologi Maklumat hendaklah menyediakan perkhidmatan membaikpulih perkakasan ICT hak milik kerajaan di Hospital Pandang yang mesti disiapkan dalam tempoh tiga (3) hari bekerja (jika tidak melibatkan sebarang penggantian komponen komputer) dari tarikh permohonan untuk dibaiki.
- 2.2. Setiap aduan hendaklah disalurkan dan direkodkan ke Sistem e-Helpdesk ICT.
- 2.3. Berikut adalah carta alir proses aduan dalam Sistem e-Helpdesk:



- 2.4. Penyelenggaraan Perkakasan ICT merangkumi;
 - a. Komputer Peribadi (PC)
 - b. Komputer Bimbit (Laptop)
 - c. Pencetak
 - d. Server
 - e. Infrastruktur di Bilik Server

2.5. Aktiviti penyelenggaraan pencegahan yang dilaksanakan adalah untuk menghapuskan punca kerosakan berpotensi dan seterusnya mencegah kerosakan daripada berlaku.

2.6. Kekerapan penyelenggaraan pencegahan adalah seperti berikut:

Bil.	Jenis Perkakasan	Kekerapan
1.	PC dan Laptop	sekali setahun
2.	UPS Bilik Server	2 kali setahun
3.	<i>Precision Aircond</i>	6 kali setahun
4.	<i>Water Leak Detector</i>	2 kali setahun
5.	<i>Fire Suppression System</i>	2 kali setahun
6.	<i>Environmental Monitoring System</i>	2 kali setahun
7.	<i>Door Access and CCTV</i>	2 kali setahun

Tertakluk kepada syarikat / kontraktor bangunan atau kontrak (jika ada)

2.7. Pengurusan katalaluan *administrator* bagi setiap PC dan laptop di Hospital Pendang adalah dibawah pengendalian Unit Teknologi Maklumat.

2.8. Sebarang instalasi perisian yang tidak berlesen tidak dibenarkan sama sekali di semua PC dan laptop di Hospital Pendang.

2.9. Setiap pengguna di lokasi penyelenggaraan perlu mengesahkan kerja- kerja penyelenggaraan yang dilakukan.

3. TATACARA PEMINJAMAN PERKAKASAN DAN PERISIAN ICT

3.1. Unit Teknologi Maklumat (ICT) menyediakan kemudahan pinjaman peralatan ICT bagi tujuan urusan rasmi sahaja.

3.2. Permohonan mestilah di buat lima (5) hari bekerja sebelum tarikh penggunaan. Sebarang kelewatan permohonan boleh menyebabkan permohonan pinjaman ditolak.

- 3.3. Permohonan pinjaman mesti dibuat melalui Borang Pinjaman Peralatan ICT (Borang KEW PA 9) berserta dengan surat/memo urusan rasmi tersebut.
- 3.4. Pihak ICT akan meluluskan permohonan pinjaman mengikut jumlah peralatan ICT yang tersedia pada masa tersebut.
- 3.5. Peminjaman peralatan ICT dari agensi luar perlu mendapat kelulusan Pengurusan Tertinggi Hospital Pendang.
- 3.6. Tempoh maksimum pinjaman peralatan adalah selama lima (5) hari bekerja sahaja. Peminjam dikehendaki mengisi borang pinjaman (KEW PA 9) semula untuk melanjutkan tempoh pinjaman.
- 3.7. Bagi peminjaman untuk kegunaan rasmi semasa waktu pejabat, peminjam atau wakil hendaklah datang sendiri untuk mengambil, mengisi borang dan memulangkan peralatan tersebut daripada/kepada pihak ICT.
- 3.8. Peminjam perlu memaklumkan kepada pihak ICT sekiranya memerlukan bantuan teknikal ICT untuk memasang dan mengambil peralatan tersebut selepas tempoh pinjaman. Sekiranya tidak dimaklumkan, peminjam adalah bertanggungjawab untuk menguruskan urusan pemasangan dan pemulangan.
- 3.9. Peminjam dikehendaki memulangkan semula peralatan yang dipinjam mengikut tarikh pinjaman. Semua peralatan yang dipinjam mestilah dipulangkan dalam tempoh waktu pejabat.
- 3.10. Bagi kegunaan di Hospital Pendang, sekiranya pemulangan tidak dapat dilakukan dalam tempoh waktu pejabat, peminjam dikehendaki memaklumkan kepada Polis Bantuan untuk menjaga peralatan ICT di lokasi tersebut.
- 3.11. Pihak ICT yang menguruskan proses pemulangan perlu memastikan peralatan dan perisian dalam keadaan baik dan begitu juga peminjam dikehendaki untuk memeriksa peralatan dan perisian yang diterima juga dalam keadaan baik.
- 3.12. Bagi pinjaman laptop, pengguna dari bahagian/unit yang telah dibekalkan kemudahan laptop perlu menggunakan laptop bahagian/unit tersebut.
bahagian/unit tidak tersedia pada tarikh yang ingin digunakan.
- 3.13. Peralatan yang dipinjam mestilah dijaga dengan rapi daripada sebarang kecurian dan kerosakan.

- 3.14. Peminjam mestilah bertanggungjawab sepenuhnya terhadap sebarang kerosakan akibat kecuaiian yang berlaku sepanjang tempoh peralatan dipinjam.
- 3.15. Sekiranya berlaku kehilangan, peminjam perlu melaporkan dengan kadar segera kepada pihak Unit Pengurusan Aset dan Unit Teknologi Maklumat serta mengambil tindakan segera berdasarkan Tatacara Pengurusan Aset Alih Kerajaan.
- 3.16. Jika penggunaan peralatan ICT memerlukan kepada pengangkutan dan kawalan keselamatan, peminjam adalah bertanggungjawab untuk menguruskan sendiri urusan tersebut.
- 3.17. Pihak ICT berhak untuk membuat pemeriksaan mengejut dari masa ke semasa untuk memastikan peralatan yang dipinjamkan berada dalam keadaan baik.
- 3.18. Data/fail peminjam adalah tanggungjawab peminjam dan hendaklah dipadam sebelum pemulangan. Data/fail sulit (*confidential*) mestilah dipadam untuk mengelakkan daripada disalahgunakan oleh pihak yang tidak bertanggungjawab. Pihak ICT tidak bertanggungjawab ke atas kehilangan atau penyalahgunaan data/fail peminjam yang di simpan dalam peralatan ICT yang dipinjamkan. Pihak ICT akan memadam data/fail tersebut selepas peralatan ICT dipulangkan semula.

4. TATACARA PENGURUSAN DAN PENGGUNAAN EMEL

- 4.1. Sistem e-mel rasmi Hospital Pendang adalah menggunakan MyGovUC 2.0 adalah Perkhidmatan Komunikasi dan Kolaboratif Bersepadu yang diuruskan secara berpusat di MAMPU. Perkhidmatan ini menggabungkan saluran-saluran komunikasi seperti e-mel, persidangan video/audio, chat dan Sistem Pengurusan Profil Pengguna (UPMS).
- 4.2. Permohonan e-mel perlu dilakukan melalui Borang Permohonan Emel MyGovUC dan akan diproses dalam tempoh satu (1-3) hari bekerja.
- 4.3. Pemilikan akaun e-mel bukan hak mutlak individu. Ia adalah kemudahan yang tertakluk kepada Hospital Pendang dan boleh ditarik balik jika penggunaannya melanggar peraturan.
- 4.4. Setiap bahagian dan unit hanya diperuntukkan satu e-mel bahagian sahaja berdasarkan keperluan dan kelulusan dari pihak pentadbir emel MAMPU. Penghantaran e-mel menggunakan e-mel bahagian perlu menjelaskan nama, jawatan dan nombor untuk dihubungi bagi mengelakkan kesamaran dalam penggunaan e-mel bahagian.
- 4.5. Katalaluan sementara perlu ditukar pada login kali pertama dan melaksanakan pengesahan serta pengaktifan 2FA (*Two Factor Authentication*).

- 4.6. Pegawai perlu menggunakan e-mel rasmi dalam semua urusan rasmi dan dilarang menggunakan alamat e-mel persendirian seperti *yahoo*, *gmail* dan sebagainya.
- 4.7. Pegawai tidak dibenarkan menggunakan e-mel rasmi untuk tujuan peribadi.
- 4.8. Pegawai adalah dilarang daripada melakukan sebarang aktiviti yang melanggar tatacara penggunaan e-mel rasmi seperti:
- Menggunakan akaun milik orang lain, berkongsi akaun atau
 - Menggunakan identiti palsu atau menyamar sebagai penghantar maklumat yang sah
 - Menggunakan e-mel untuk tujuan komersial atau politik.
 - Menghantar dan memiliki bahan-bahan yang salah di sisi undang-undang seperti bahan lucah, perjudian dan jenayah.
 - Menghantar dan melibatkan diri dalam e-mel yang berunsur hasutan, e-mel sampah, e-mel bom, e-mel spam, fitnah, ciplak atau aktiviti-aktiviti lain yang ditegah oleh undang-undang kerajaan Malaysia.
 - Menyebarkan kod perosak seperti virus, worm, trojan horse dan trap door yang boleh merosakkan sistem komputer dan maklumat pengguna lain.
 - Menghantar semula e-mel yang gagal sampai ke destinasi sebelum menyiasat punca kejadian.
 - Membenarkan pihak ketiga untuk menjawab e-mel kepada penghantar asal bagi pihaknya.
- 4.9. Setiap pegawai bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing bagi memastikan e-mel yang disimpan tidak melebihi saiz *mailbox* yang telah diperuntukkan. Sekiranya kapasiti telah digunakan sepenuhnya, e-mel masuk yang baru tidak akan diterima oleh sistem.
- 4.10. E-mel akan dihapus dalam tempoh 90 hari selepas pegawai dan kakitangan meletak jawatan, berpindah kementerian, bersara atau meninggal dunia juga termasuk bagi e-mel yang dikenalpasti tidak aktif.

5. TATACARA PENGGUNAAN INTERNET

Berikut adalah tatacara yang mesti diikuti dalam menggunakan Internet:

- 5.1. Hak Akses Pengguna: Hak akses hendaklah dilihat sebagai satu kemudahan yang disediakan oleh Kerajaan untuk melicinkan pentadbiran atau memperbaiki perkhidmatan yang disediakan. Pengguna harus mengambil maklum bahawa semua aset ICT di bawah kawalannya (termasuk maklumat) adalah hak milik Kerajaan.

- 5.2. Memilih Laman: Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan.
- 5.3. Pengesahan Maklumat: Bahan yang diperolehi dari Internet perlulah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah juga dinyatakan.
- 5.4. Muat Naik Bahan: Bahan rasmi yang hendak dimuat naik ke Internet hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik.
- 5.5. Muat Turun Bahan: Tindakan memuat turun hanya dibenarkan ke atas bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh jabatan sahaja.
- 5.6. Perbincangan Awam: Hanya pegawai yang mendapat kebenaran sahaja boleh melibatkan diri dan menggunakan kemudahan ini. Kandungan perbincangan awam seperti forum, newsgroup dan bulletin board mestilah mendapat pengesahan daripada Ketua Jabatan tertakluk kepada dasar dan tatacara yang telah ditetapkan. Perlu diingat bahawa setiap maklumat yang dikongsi melambangkan imej Kerajaan. Dengan sebab itu, setiap pengguna mestilah bertindak dengan bijaksana, jelas dan berupaya mengekalkan konsistensi dan keutuhan maklumat berkenaan.
- 5.7. Pegawai dan kakitangan Hospital Pengang adalah DILARANG daripada melakukan sebarang aktiviti yang melanggar tatacara penggunaan Internet seperti:
 - a. memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen
 - b. menyediakan dan menghantar maklumat berulang-ulang berupa gangguan
 - c. memuat naik, memuat turun, menyimpan dan menghantar sebarang bentuk maklumat atau perkara rahsia rasmi yang mesti diberi perlindungan untuk kepentingan keselamatan yang dikelaskan mengikut pengelasannya sama ada Terhad, Sulit, Rahsia atau Rahsia Besar.
 - d. menyediakan, memuat naik, memuat turun dan menyimpan maklumat Internet yang melibatkan sebarang pernyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan imej Kerajaan
 - e. melayari, menyediakan, memuat naik, memuat turun dan menyimpan material, teks ucapan, imej atau bahan-bahan yang mengandungi unsur-unsur lucah;
 - f. memuat naik, memuat turun dan menyimpan gambar atau teks yang bercorak penentangan yang boleh membawa keadaan huru-hara dan menakutkan pengguna Internet yang lain;

- g. memuat turun, menyimpan dan menggunakan perisian berbentuk hiburan atas talian seperti permainan elektronik, video dan lagu;
- h. memuat naik, memuat turun, menghantar dan menyimpan kad elektronik, video, lagu dan kepingan fail melebihi saiz 2 megabait yang boleh mengakibatkan kelewatan perkhidmatan dan operasi sistem rangkaian komputer;
- i. menyalahgunakan kemudahan perbincangan awam atas talian seperti forum, newsgroup dan bulletin board;
- j. menggunakan kemudahan chatting melalui Internet;
- k. menggunakan kemudahan Internet untuk tujuan peribadi;
- l. menjalankan aktiviti-aktiviti komersial dan politik;
- m. melakukan aktiviti jenayah seperti menyebarkan bahan yang membabitkan perjudian, senjata dan aktiviti penganas;
- n. menggunakan kemudahan modem peribadi untuk membuat capaian terus ke Internet.

6. TATACARA PENGGUNAAN DAN PENGURUSAN RANGKAIAN

- 6.1. Unit Teknologi Maklumat adalah bertanggungjawab dalam menyelenggara rangkaian setempat, talian internet dan perkhidmatan talian Kerajaan yang diberi melalui Projek MyGovNet.
- 6.2. Perkakasan rangkaian di Hospital Pandang merangkumi peralatan seperti berikut:
 - a. *Firewall*
 - b. *Switches*
 - c. *Server*
 - d. *Router*
 - e. *Node* rangkaian
 - f. *Wireless Access Point*
 - g. Infrastruktur kabel rangkaian
 - h. *Network Rack*
- 6.3. Semua peralatan rangkaian hendaklah diletakkan di tempat yang dikhususkan contohnya dalam rak atau di bilik *server*. Sebarang perubahan lokasi peralatan rangkaian perlu mendapatkan kelulusan ICT Hospital Pandang.
- 6.4. Sebarang penyambungan rangkaian tambahan perlu mendapat kebenaran dan dimaklumkan terlebih dahulu kepada ICT Hospital Pandang dan mematuhi piawaian yang ditetapkan.

- 6.5. Semua pengguna yang menggunakan peralatan ICT peribadi perlu merujuk kepada ICT Hospital Pendang serta dilengkapi dengan perisian antivirus yang terkini sebelum dibenarkan akses ke rangkaian Hospital Pendang. Sebarang kerosakan dan serangan virus ke atas peralatan ICT peribadi adalah di bawah tanggungjawab pengguna.
- 6.6. Pemasangan *wireless access point* peribadi perlu merujuk kepada ICT Hospital Pendang bagi mengelakkan sebarang gangguan terhadap rangkaian sedia ada. Secara dasarnya, pemasangan *wireless access point* peribadi adalah tidak dibenarkan kecuali atas justifikasi yang kukuh. Pihak ICT Hospital Pendang berhak untuk menanggalkan pemasangan *wireless access point* yang dipasang tanpa kebenaran ICT Hospital Pendang.
- 6.7. *Telecommunication Room (TCR)* hanya menempatkan peralatan ICT dan peralatan lain dengan kebenaran ICT Hospital Pendang.
- 6.8. Capaian internet ke laman-laman web rasmi kerajaan (.gov) adalah melalui talian MyGovNet.
- 6.9. Capaian *remote access* perlu mendapat kebenaran dari ICT Hospital Pendang dan direkodkan.
- 6.10. Semua kabel rangkaian hendaklah dipasang dengan kemas seperti di bawah lantai atau melalui *conduit*, yang mana bersesuaian.
- 6.11. Semua trafik keluar dan masuk hendaklah melalui satu *gateway* sahaja iaitu *firewall* yang dikawal oleh ICT Hospital Pendang.
- 6.12. Sebarang perisian yang boleh mencerooboh keselamatan rangkaian dan komunikasi tidak dibenarkan penggunaannya sama sekali melainkan mendapat kelulusan ICT Hospital Pendang.
- 6.13. Penggunaan perisian *sniffer* atau *network analyzer* tidak dibenarkan.

7. PENGGUNAAN DAN PENGURUSAN SISTEM APLIKASI

Perkara-perkara berhubung sistem aplikasi di Hospital Pendang yang perlu dipatuhi adalah seperti berikut:

- a. Capaian sistem aplikasi adalah terhad kepada pengguna dan tujuan yang dibenarkan;

- b. Pengguna bertanggungjawab kepada akses yang diberikan dan adalah dilarang mendedahkan Nama Pengguna dan Kata laluan kepada individu lain;
- c. Pentadbir Sistem berhak menarik balik kemudahan akses atas sebab-sebab berikut:
 - i. Bertukar bidang tugas kerja;
 - ii. Bertukar ke agensi lain;
 - iii. Bersara; atau
 - iv. Ditamatkan perkhidmatan.
- d. Pengguna bertanggungjawab ke atas sensitiviti maklumat yang dicapai di dalam sistem aplikasi;
- e. Pentadbir sistem bertanggungjawab terhadap pengurusan pangkalan data, pengujian aplikasi, perubahan versi dan penyimpanan kod sumber mengikut garis panduan yang telah ditetapkan;
- f. Semua sistem aplikasi yang diperolehi untuk atau bagi pihak KKM atau semua perisian yang dibangunkan oleh pegawai untuk tujuan penyelidikan atau pentadbiran adalah menjadi hakmilik KKM; dan
- g. Penyenggaraan Sistem adalah meliputi penyenggaraan aplikasi, pangkalan data dan komputer pelayan dan dilaksanakan dari semasa ke semasa mengikut keperluan

8. PENGURUSAN BILIK SERVER

8.1. Polisi ini menjelaskan mengenai pematuhan terhadap aspek fizikal dan keselamatan terhadap bilik server Hospital Pendang selaras dengan pematuhan terhadap peraturan yang telah ditetapkan dalam Dasar Keselamatan ICT KKM Versi 5.0 dalam memperkukuhkan keselamatan dan ketersediaan Bilik Server di Hospital Pendang.

8.2. Bilik server Hospital Pendang mempunyai kemudahan sistem pengurusan keselamatan fizikal dan infrastruktur seperti berikut:

- a. *In-Row Air Conditioning*
- b. *Uninterruptable Power Supply*
- c. *Water Leak Detection System*
- d. *Fire Suppression System*
- e. *High Sensitivity Smoke Detection System*
- f. *Environment Monitoring System*
- g. *Door Access dan CCTV*

8.3. Bilik server Hospital Pendang dilengkapi dengan sistem penghawa dingin yang beroperasi 24 jam secara bergilir dengan suhu di antara 19°C hingga 24°C dengan kelembapan pada tahap 60% hingga 70%.

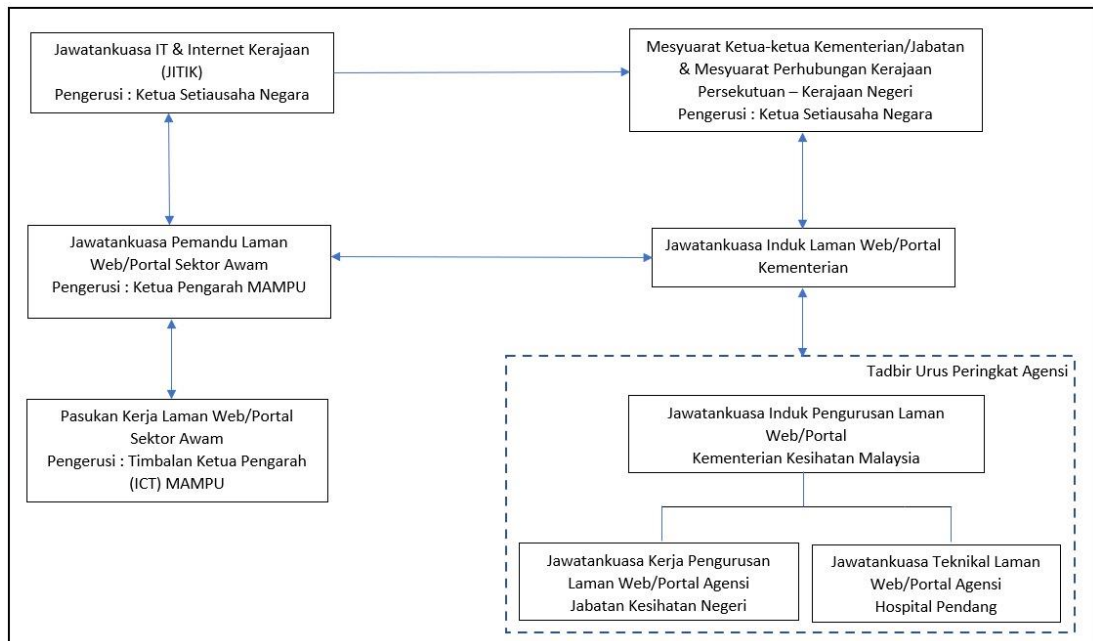
- 8.4. Laluan yang menghubungkan bilik server dengan ruang-ruang atau bilik- bilik lain seperti ruang penyimpanan dan kawasan luar bangunan tidak boleh mempunyai sebarang halangan.
- 8.5. Barang-barang yang tidak digunakan tidak boleh ditinggalkan dan dilarang membawa masuk makanan ke dalam bilik server. Contohnya: kotak peralatan, bahan api yang mudah terbakar, plastik makanan, cawan kertas dan sebagainya.
- 8.6. Bagi memastikan keselamatan bilik server, perkara-perkara berikut mestilah dipatuhi:
- a. Kawalan akses ke bilik server perlulah mempunyai ciri -ciri keselamatan seperti kata laluan dan penggunaan sistem elektronik kad pintar dan mekanikal;
 - b. Kebenaran masuk ke kawasan persekitaran bilik server hendaklah diiringi oleh sekurang-kurangnya seorang Pentadbir Sistem atau kakitangan teknikal yang dilantik bagi menentukan dan mengawal selia penugasan yang diperlukan;
 - c. Aktiviti yang dilaksanakan oleh Pentadbir Sistem atau Pembekal hendaklah direkodkan ke dalam buku log yang disediakan. Sebarang pemindahan maklumat daripada bilik server hendaklah dipohon dan mendapat kebenaran daripada pemilik data (*data owner*) dan Pentadbir Sistem masing-masing;
 - d. Bilik Server hendaklah mempunyai sistem pengudaraan (*ventilation*) yang mencukupi dan alat penghawa dingin yang berupaya mengawal kelembapan udara bagi mengelak kerosakan komponen elektronik pada perkakasan komputer berkenaan. Penggunaan lantai di dalam bilik server perlu dilaksanakan secara bertingkat (*raised floor*);
 - e. Sistem pengaliran air yang sempurna juga penting bagi bilik server untuk mengelak banjir. Pemeriksaan terhadap bangunan yang berkenaan hendaklah dilaksanakan setiap 6 bulan oleh penyelia bangunan yang bertauliah atau dilantik; dan
 - f. Penggunaan kamera litar adalah perlu dalam memastikan kawalan keselamatan bilik server.

9. PEMBANGUNAN DAN PENGURUSAN LAMAN WEB

- 9.1. Tadbir urus laman web Hospital Pendang khususnya yang berkaitan dengan kandungan diselaraskan melalui Jawatankuasa Pengurusan Laman Web Hospital Pendang berdasarkan

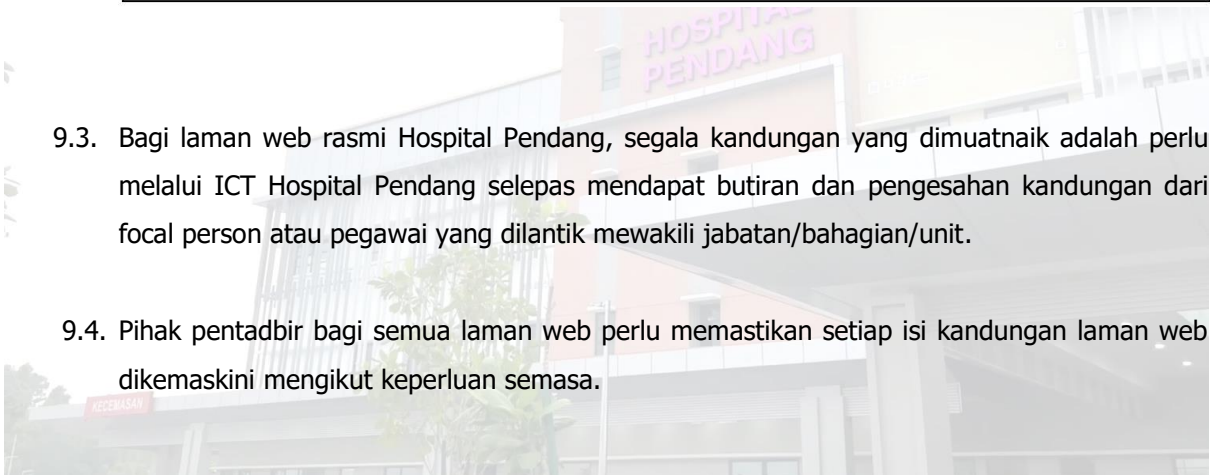
Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 Pengurusan Laman Web Agensi Sektor Awam.

9.2. Berikut adalah rajah yang menunjukkan kedudukan tadbir urus laman web Hospital Pendang:



9.3. Bagi laman web rasmi Hospital Pendang, segala kandungan yang dimuatnaik adalah perlu melalui ICT Hospital Pendang selepas mendapat butiran dan pengesahan kandungan dari focal person atau pegawai yang dilantik mewakili jabatan/bahagian/unit.

9.4. Pihak pentadbir bagi semua laman web perlu memastikan setiap isi kandungan laman web dikemaskini mengikut keperluan semasa.



PEMAKAIAN

Polisi ICT Hospital Pendang adalah terpakai kepada semua pengguna sumber ICT yang terdiri daripada kakitangan tetap dan kontrak, kontraktor dan mana-mana pihak yang mempunyai ikatan kontrak atau hubungan, sama ada secara bertulis atau tidak dengan Hospital Pendang .

Polisi ini adalah terpakai kepada semua pengoperasian ICT Hospital Pendang selagi mana ianya tidak bertentangan dengan mana-mana peruntukan undang-undang dan peraturan yang terpakai di KKM dan Kerajaan.

Sekiranya terdapat perbezaan Polisi ICT Hospital Pendang dengan mana-mana peruntukan undang-undang, maka peruntukan undang-undang tersebut adalah terpakai dan Polisi ini hendaklah dipinda selaras dengan perubahan, pindaan kepada undang-undang dan peraturan yang mengikat Hospital Pendang; dan

Polisi ICT Hospital Pendang ini boleh ditambah baik dan dipinda dari semasa ke semasa selaras dengan fungsi dan kuasa Hospital Pendang serta arahan semasa dari KKM dan Kerajaan.

PENGECUALIAN

Sebarang pengecualian daripada mana-mana peruntukan dalam Garis Panduan ini hendaklah mendapat pertimbangan dan kelulusan Pengurusan Tertinggi Hospital Pendang dan Unit Teknologi Maklumat (ICT) Hospital Pendang.

TARIKH KUATKUASA

Polisi ICT Hospital Pendang adalah berkuat kuasa daripada tarikh ia diterbitkan.