Kementerian Kesihatan Malaysia
Hospital Tuanku Jaafar Seremban

POLISI ICT
HOSPITAL TUANKU JAAFAR, SEREMBAN

DISEDIAKAN OLEH	DISEMAK OLEH
---------- RAIHAYU BINTI ABD RAHMAN KETUA PENOLONG PENGARAH (ICT) UNIT TEKNOLOGI MAKLUMAT DAN KOMUNIKASI TARIKH: 13/8/2026	---------- DR. ZUHAIDA BINTI CHE EMBI TIMBALAN PENGARAH PERUBATAN I TARIKH: 13/8/2026
DISAHKAN OLEH	
---------- DATO' DR. ZALEHA BINTI MD NOOR PENGARAH HOSPITAL TARIKH: 13/8/2026	

TARIKH KEMASKINI TERDAHULU :
TARIKH KEMASKINI TERKINI :

HOSPITAL TUANKU JA'AFAR
SEREMBAN

POLISI ICT

UNIT TEKNOLOGI MAKLUMAT & KOMUNIKASI
HOSPITAL TUANKU JA'AFAR
SEREMBAN

HOSPITAL TUANKU JA'AFAR, SEREMBAN
Jalan Rasah, 70300 Seremban,
Negeri Sembilan Darul Khusus.

06-7684000

icthjs@moh.gov.my

UTMK
Unit Teknologi Maklumat & Komunikasi

KAWALAN DOKUMEN

No. Versi	Tarikh	Ringkasan Pindaan	Penyedia
1.0			

ISI KANDUNGAN

SENARAI LAMPIRAN

Lampiran A : Surat Akuan Pematuhan Polisi ICT HTJS (HTJS/ICT/BRG 023)

Lampiran B : Surat Lantikan CDO

Lampiran C : Surat Lantikan ICTSO

Lampiran D : Senarai Borang

1. Borang Pendaftaran ID (HTJS/ICT/BRG 001 Pin.1/25)
2. Borang SPP Issue Log (HTJS/ICT/BRG 002 Pin.1/25)
3. Borang Pengesahan ICT (HTJS/ICT/BRG 003)
4. Borang Pengesahan Latihan ICT bagi Kakitangan HTJS (HTJS/ICT/BRG 004)
5. Borang Penilaian Prestasi Pembekal (HTJS/ICT/BRG 005)
6. Borang Permohonan Pembangunan Sistem *Inhouse* (HTJS/ICT/BRG 006)
7. Borang Penyelenggaraan Sistem *Inhouse* (HTJS/ICT/BRG 007 Pin.1/25)
8. Borang Log Pengurusan *Server* (HTJS/ICT/BRG 008)
9. Borang Log *Backup* Sistem dan Pangkalan Data Sistem Inhouse (HTJS/ICT/BRG 009)
10. Borang *Restore* Aplikasi dan Pangkalan Data Sistem Inhouse (HTJS/ICT/BRG 010)
11. Borang Pengurusan Kawalan Perubahan (HTJS/ICT/BRG 011)
12. Borang Kemaskini Laman Web HTJS (HTJS/ICT/BRG 012 Pin.1/25)
13. Borang Permohonan Akses Disiplin dan *Role* Sistem (HTJS/ICT/BRG 013 Pin.1/25)
14. Borang Tempahan Makmal ICT Blok Cempaka (HTJS/ICT/BRG 014)
15. PKP Borang Pendaftaran Pesakit (Umum) (HTJS/ICT/BRG 015)

16. PKP Borang Pendaftaran Pesakit Unit Daftar Masuk (UDM) (HTJS/ICT/BRG 016)
17. PKP *Dispatched List Laboratory Order* (HTJS/ICT/BRG 017)
18. PKP Borang Senarai Pemeriksaan Radiologi (HTJS/ICT/BRG 018)
19. Borang Pengujian Penerimaan Pengguna (UAT) (HTJS/ICT/BRG 019)
20. Borang Pengujian Penerimaan Akhir (FAT) (HTJS/ICT/BRG 020)
21. Borang Penyerahan Sistem Aplikasi (HTJS/ICT/BRG 021)
22. Borang Penamatan/Penangguhan Sistem Aplikasi (HTJS/ICT/BRG 022)

GLOSARI

Bil	Perkataan	Tafsiran
1.	Antivirus	Perisian keselamatan yang berfungsi untuk mengimbas, mengesan, menghalang dan membuang perisian hasad (malware) termasuk virus dan lain-lain ancaman keselamatan dari sistem komputer, media storan atau rangkaian.
2.	*Backup*	Proses menyalin data atau sistem komputer ke lokasi atau media simpanan lain dengan tujuan untuk pemulihan *(recovery)* sekiranya data asal hilang, rosak, atau tidak dapat diakses
3.	BYOD	*Bring Your Own Device* (BYOD) – Bawa Peranti Anda Sendiri Dasar yang membenarkan pengguna menggunakan peranti peribadi seperti komputer riba atau telefon pintar untuk mengakses sistem dan data organisasi dengan kawalan keselamatan tertentu.
4.	CDO	*Chief Digital Officer* – Ketua Pegawai Digital Pegawai yang bertanggungjawab merancang dan melaksana strategi dalam memacu inovasi teknologi digital bagi meningkatkan penyampaian perkhidmatan, mengoptimumkan penggunaan data dan analitik, memastikan keselamatan siber, dan menyelaras perubahan budaya serta pengurusan sumber manusia untuk memastikan organisasi kekal kompetitif dan relevan dalam era digital yang pesat berkembang.
5.	ICT	*Information and Communication Technology* (ICT) – Teknologi Maklumat dan Komunikasi Merujuk kepada sistem, peralatan, perisian, aplikasi dan perkhidmatan yang digunakan untuk mengurus,

Bil	Perkataan	Tafsiran
		memproses, menyimpan, menghantar atau menerima maklumat secara elektronik.
6.	ICTSO	*ICT Security Officer* – Pegawai Keselamatan ICT Pegawai yang bertanggungjawab melaksanakan polisi keselamatan siber, menguruskan infrastruktur keselamatan, memantau keselamatan, mengesan pencerobohan, menilai ancaman, menguruskan insiden serta melatih pegawai mengenai langkah perlindungan keselamatan dalam memastikan pematuhan kepada undang-undang dan peraturan keselamatan siber
7.	Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
8.	JICT	Jawatankuasa ICT adalah jawatankuasa dalaman yang ditubuhkan bagi menyelaras perancangan, pelaksanaan, pemantauan dan penilaian aktiviti ICT serta memastikan pematuhan terhadap dasar dan pelan strategik ICT.
9.	Kontraktor	Seseorang atau kumpulan orang yang dibenarkan membekal sama ada perkhidmatan, peralatan ICT atau aplikasi di HTJS
10.	LAN	*Local Area Network* Rangkaian komputer yang menghubungkan peranti dalam kawasan geografi yang terhad — seperti dalam rumah, pejabat, bangunan, atau kampus.
11.	Meja Bantuan ICT	Khidmat sokongan teknikal untuk pengguna melaporkan sebarang masalah berkaitan peralatan ICT dan aplikasi di HTJS
12.	Pelan Kesinambungan Perkhidmatan	Pelan Kesinambungan Perkhidmatan (PKP) merujuk kepada pelan atau perancangan pengurusan kesinambungan perkhidmatan. Perancangan ini yang

Bil	Perkataan	Tafsiran
	(PKP)	meliputi segala sumber, proses, peranan dan tanggungjawab semua pihak terlibat yang diperlukan sebelum, semasa dan selepas sesuatu gangguan kepada sistem penyampaian perkhidmatan perlu didokumenkan, diuji dan dikaji semula secara berkala dan dilaksanakan apabila berlaku gangguan. Di samping itu, tindakan dilaksanakan untuk segera membaik pulih pelaksanaan fungsi-fungsi normal agensi dalam tempoh yang ditetapkan.
13.	Pengguna	Mana-mana kakitangan HTJS yang menggunakan perkhidmatan ICT HTJS
14.	Pentadbir E-mel	Pegawai yang mengurus perkhidmatan e-mel
15.	Pentadbir Laman Web	Pegawai teknikal yang menyelenggara laman web
16.	Pentadbir Rangkaian	Pegawai yang mengurus rangkaian dan bertanggungjawab untuk memasang, memantau aktiviti rangkaian, menyelesaikan masalah dan menaik taraf infrastruktur rangkaian, termasuk komponen peralatan dan perisian rangkaian.
17.	Pentadbir *Server*	Pegawai teknikal yang mengawasi *server* komputer
18.	Pentadbir Sistem	Pegawai yang menguruskan aplikasi atau perisian tertentu dalam jabatan. Bertanggungjawab memasang, mengemas kini dan menyelenggara aplikasi yang diberikan.
19.	Penyelaras ICT	Pegawai ICT yang dilantik untuk bertanggungjawab mengurus dan menyelaras infrastruktur ICT jabatan / unit.
20.	Peralatan	Merangkumi semua jenis peralatan dan kelengkapan ICT seperti yang disenaraikan di dalam Sistem Pengurusan Aset Alih (SPA).
21.	Perisian	Merangkumi semua jenis perisian sistem, perisian aplikasi dan lesen perisian (pembelian dan pembaharuan). Perisian

Bil	Perkataan	Tafsiran
		sistem merangkumi sistem operasi, pangkalan data dan perisian bagi membangunkan sistem. Perisian aplikasi ialah perisian yang digunakan untuk menyokong kerja-kerja harian dalam urusan dan pentadbiran pejabat serta pengajaran dan pembelajaran.
22.	*Restore*	Proses memulihkan data, sistem, atau perisian kepada keadaan asal atau keadaan sebelumnya selepas berlaku kehilangan data, kerosakan sistem, serangan virus, atau kegagalan teknikal, biasanya menggunakan salinan *backup*.
23.	*Router*	Peralatan rangkaian yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan.
24.	*Server*	Merujuk kepada sistem komputer (atau program komputer) yang menyediakan sumber, data, perkhidmatan, atau program kepada komputer lain, yang dikenali sebagai "klien," melalui rangkaian.
25.	Sistem Aplikasi	Semua sistem
26.	SLA	*Service Level Agreement* (SLA) – Perjanjian peringkat perkhidmatan Perjanjian antara penyedia perkhidmatan dan pelanggan. Aspek tertentu perkhidmatan – kualiti, ketersediaan, tanggungjawab – dipersetujui antara penyedia perkhidmatan dan pengguna perkhidmatan. Komponen yang paling biasa dalam SLA ialah perkhidmatan perlu diberikan kepada pelanggan seperti yang dipersetujui dalam kontrak.
27.	*Switch*	Peranti rangkaian yang berfungsi untuk menghubungkan beberapa peranti dalam satu rangkaian tempatan (LAN) dan menghantar data secara langsung kepada peranti

Bil	Perkataan	Tafsiran
		yang dituju berdasarkan alamat MAC *(Media Access Control)*
28.	UPS	*Uninterupted Power Supply* Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung
29.	WAN	*Wide Area Network* Rangkaian komputer berskala besar yang menghubungkan dua atau lebih rangkaian tempatan (LAN) merentasi kawasan geografi yang luas, seperti antara bandar, negeri atau negara, menggunakan talian komunikasi awam atau persendirian.
30.	WAP	*Wireless Access Point* Peranti rangkaian yang membolehkan peranti tanpa wayar seperti telefon pintar, komputer riba dan *tablet* bersambung ke rangkaian komputer melalui Wi-Fi, serta menghubungkan peranti tersebut ke rangkaian berwayar (LAN).

A TADBIR URUS ICT HTJS

1 PENGENALAN

Polisi ICT Hospital Tuanku Ja'afar, Seremban (HTJS) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi semasa menggunakan infrastruktur teknologi maklumat dan komunikasi (ICT). Polisi ini juga menerangkan tanggungjawab pengguna dalam melindungi kemudahan ICT yang disediakan di HTJS. Polisi ini perlu dibaca bersama dengan **Polisi Keselamatan Siber Versi 1.0 Kementerian Kesihatan Malaysia (PKS KKM)**.

2 TUJUAN

Tujuan Polisi ICT ini adalah seperti berikut:

i. Mewujudkan dokumen rujukan hidup yang relevan dengan persekitaran perkhidmatan kesihatan semasa;
ii. Memastikan infrastruktur ICT dan rangkaian menyokong adaptasi teknologi baharu dan dikawal selia dengan baik;
iii. Memastikan isu-isu kerahsiaan, keselamatan, bidang kuasa dan etika pengguna ICT dilindungi dan diuruskan melalui saluran yang betul;
iv. Menyediakan rangka-kerja dan sumber rujukan yang lengkap mengenai hal ehwal ICT;
v. Mengawal sumber-sumber ICT supaya dilindungi secukupnya daripada perbuatan salahguna atau kecurian / kehilangan;
vi. Memastikan kelancaran operasi harian sumber-sumber ICT;
vii. Meminimumkan risiko insiden ke atas sumber-sumber ICT;
viii. Melindungi kepentingan pihak-pihak yang bergantung kepada sumber-sumber ICT daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan dan aksesibiliti sumber-sumber ICT; dan
ix. Mendukung usaha pendigitalan perkhidmatan kerajaan dengan memastikan penggunaan sistem aplikasi secara *cloud* dan sistem aplikasi

sokongan yang disediakan oleh Kementerian Kesihatan Malaysia (KKM), Jabatan Digital Negara (JDN), Jabatan Perkhidmatan Awam (JPA) dan Kementerian Kewangan.

3 PRINSIP

Prinsip-prinsip yang menjadi asas kepada Polisi ICT HTJS dan perlu dipatuhi adalah seperti berikut:

3.1 Capaian Atas Dasar Perlu

Capaian kepada sumber ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar 'perlu mengetahui' sahaja. Capaian akan hanya dibenarkan sekiranya peranan atau tanggungjawab tugasnya memerlukan penggunaan sumber maklumat elektronik.

3.2 Kebenaran Capaian

Mematuhi prinsip bahawa pengguna boleh diberi kebenaran capaian kategori maklumat tertentu setelah siasatan menunjukkan tiada sebab atau faktor untuk menghalang pengguna tersebut daripada berbuat demikian.

3.3 Hak Capaian Minimum

Hak capaian kepada pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan / atau melihat sahaja. Kelulusan khas daripada pentadbir sistem aplikasi adalah diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu data atau maklumat.

3.4 Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap sumber ICT di bawah jagaannya atau yang digunakannya. Tanggungjawab ini hendaklah dinyatakan dengan jelas sejajar dengan tahap sensitiviti sesuatu sumber ICT berkenaan. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna tersebut dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuk, tetapi tidak terhad kepada:

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

3.5 Pematuhan

Pematuhan adalah merupakan prinsip penting dalam menghindar dan mengesan sebarang perlanggaran Polisi. Pematuhan kepada Polisi ICT HTJS boleh dicapai melalui tindakan-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. Melaksanakan program pemantauan keselamatan secara berterusan untuk memastikan standard, prosedur dan garispanduan keselamatan dipatuhi; dan
iii. Menguatkuasakan amalan melapur sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan.

Aktiviti-aktiviti berikut adalah dilarang keras di bawah Polisi ini:

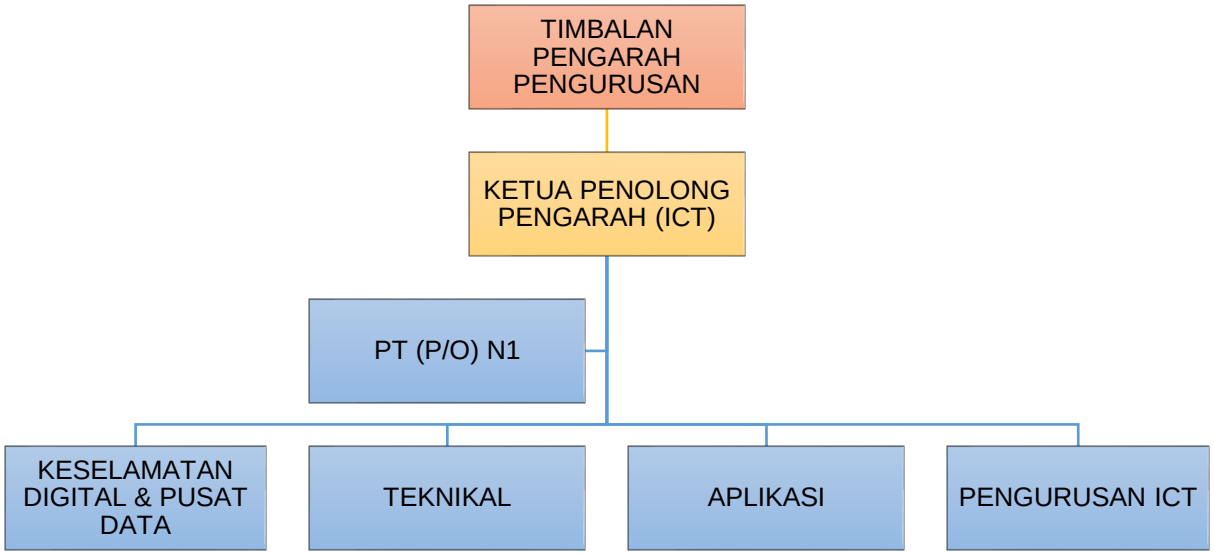
i. Mengganggu, merosak atau menyekat sumber-sumber ICT HTJS;
ii. Dengan sengaja menyebarkan sebarang virus komputer, worms atau perisian-perisian lain yang merosakkan (malicious softwares);
iii. Cuba mengakses atau mengeksploit sumber-sumber ICT yang mana dia tidak diberi kebenaran untuk berbuat demikian;
iv. Dengan sengaja membolehkan tahap-tahap akses atau eksploitasi sumber-sumber ICT yang tidak sepatutnya, oleh orang lain;
v. Memuat turun data/maklumat yang sensitif atau sulit ke komputer-komputer yang tidak dikonfigurasikan secukupnya untuk melindungi dari akses yang tidak dibenarkan; dan
vi. Menyebarkan sebarang data atau maklumat yang dia tidak mempunyai hak untuk berbuat demikian.

3.6 Pemulihan

Pemulihan sistem aplikasi dan rangkaian di HTJS amatlah perlu untuk memastikan kebolehsediaan dan kebolehcapaian sumber-sumber ICT dan sumber-sumber maklumat elektronik. Matlamat utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan.

4 STRUKTUR ORGANISASI

Berikut adalah struktur organisasi UTMK:



Berikut adalah maklumat perjawatan dan sumber sedia ada:

Bil	Jawatan / Gred	Bilangan
1	Ketua Penolong Pengarah (ICT) F12	1
2	Pegawai Teknologi Maklumat F10	2
3	Pegawai Teknologi Maklumat F9/F10	4
4	Penolong Pegawai Teknologi Maklumat Kanan FA7	1
5	Penolong Pegawai Teknologi Maklumat FA6	1
6	Penolong Pegawai Teknologi Maklumat FA5	3
7	Juruteknik Komputer (Kanan) FT2	1
8	Juruteknik Komputer FT1	6
9	Pembantu Tadbir (Pengoperasian) N1	1
	JUMLAH	**20**

5 SKOP PERKHIDMATAN

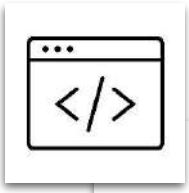
Polisi ini merangkumi skop perkhidmatan seperti di carta fungsi UTMK seperti berikut:

KESELAMATAN DIGITAL & PUSAT DATA

- Pengurusan Keselamatan Digital
- Pengurusan Pusat Data

TEKNIKAL

- Pengurusan Meja Bantuan *(Helpdesk)* ICT
- Khidmat Sokongan Teknikal ICT
- Pengurusan Rangkaian
- Pengurusan Aset ICT



APLIKASI

- Pengurusan Sistem Aplikasi
- Pengurusan ID Sistem Aplikasi dan e-Mel Rasmi
- Pengurusan Latihan Pemantapan Penggunaan Sistem Aplikasi

PENGURUSAN ICT

- Pengurusan Laman Web HTJS
- Pengurusan Kursus ICT
- Pengurusan Dokumentasi ICT
- Pengurusan Kontrak Perkhidmatan ICT
- Khidmat Multimedia HTJS
- Hebahan E-Mel dan Memo

6 OBJEKTIF

Sistem Aplikasi & Rangkaian: Memastikan tahap ketersediaan *(uptime)* rangkaian setempat (LAN) dan sistem aplikasi utama hospital (HIS) berada pada tahap **minimum 98% setiap bulan**.

Sokongan Teknikal (Helpdesk): Menyelesaikan aduan kerosakan perkakasan dan gangguan sistem komputer berdasarkan piagam pelanggan UTMK

Keselamatan Siber: Mencapai **sasar *zero-breach* (sifar pencerobohan data)** dengan memastikan tahap persekitaran keselamatan berada pada tahap optimum.

Latihan Kakitangan: Menganjurkan sekurang-kurangnya **3 hingga 4 sesi latihan/taklimat ICT setahun** untuk meningkatkan literasi digital dan kesedaran keselamatan siber dalam kalangan kakitangan klinikal dan pengurusan hospital.

7 PIAGAM PELANGGAN

Unit Teknologi Maklumat & Komunikasi (UTMK) HTJS komited menyediakan perkhidmatan ICT yang cekap, selamat dan berkesan bagi menyokong penyampaian perkhidmatan kesihatan berkualiti.

Kami berjanji untuk:

Memastikan rangkaian dan sistem aplikasi utama hospital (HIS) berada pada tahap ketersediaan sekurang-kurangnya 98% setiap bulan

Memastikan setiap aduan, permohonan dan gangguan ICT diberi tindakan serta diselesaikan dalam tempoh yang ditetapkan.

Melaksanakan kawalan keselamatan ICT secara berterusan bagi melindungi data, sistem dan aset ICT hospital daripada ancaman siber.

Melaksanakan penyelenggaraan berkala, pengurusan sandaran data dan langkah pemulihan bagi memastikan perkhidmatan ICT sentiasa tersedia.

Menganjurkan sekurang-kurangnya 3 hingga 4 sesi latihan/taklimat ICT setahun bagi meningkatkan kemahiran pengguna dan kesedaran keselamatan siber.

Memastikan setiap perkhidmatan ICT disampaikan secara responsif, telus dan berorientasikan kepuasan pengguna.

8 PERANAN

8.1 KETUA PEGAWAI DIGITAL (*CHIEF DIGITAL OFFICER* – CDO)

Tanggungjawab CDO adalah termasuk tetapi tidak terhad kepada:

i. Menetapkan hala tuju dan strategi pendigitalan hospital;
ii. Menyelaras inisiatif transformasi digital dan inovasi ICT;
iii. Memastikan pelaksanaan ICT selaras dengan keperluan operasi, keselamatan maklumat dan pematuhan dasar Kerajaan; dan
iv. Memberi nasihat strategik kepada pihak pengurusan berkaitan teknologi digital.

8.2 PEGAWAI KESELAMATAN ICT (*ICT SECURITY OFFICER* – ICTSO)

Tanggungjawab CDO adalah termasuk tetapi tidak terhad kepada:

i. Menyelaras pelaksanaan dasar dan kawalan keselamatan ICT hospital;
ii. Mengenal pasti, menilai dan memantau risiko keselamatan maklumat;
iii. Menyelaras pengurusan insiden keselamatan ICT;
iv. Memantau pematuhan audit keselamatan ICT dan ISMS; dan
v. Bertindak sebagai pegawai rujukan keselamatan ICT hospital.

8.3 PENGGUNA

8.3.1 TATACARA KESELAMATAN PEGAWAI MASUK, BERTUKAR DAN TAMAT PERKHIDMATAN HTJS

Tujuan tatacara ini adalah bagi memastikan semua pegawai yang melapor diri, bertukar masuk, bertukar keluar atau tamat perkhidmatan di HTJS mematuhi keperluan keselamatan siber, melindungi maklumat rasmi serta memastikan kawalan capaian dilaksanakan secara teratur dan selamat.

Tatacara ini terpakai kepada:

i. Semua pegawai tetap, kontrak dan sambilan HTJS
ii. Pegawai yang bertukar masuk atau keluar
iii. Pegawai yang tamat perkhidmatan

8.3.1.1 Pegawai Melapor Diri (Baharu / Bertukar Masuk)

i. Pegawai WAJIB membaca dan memahami Polisi ICT HTJS dan PKS KKM.
ii. Pegawai WAJIB mengisi dan menandatangani semua dokumen iaitu:
    - Surat Akuan PKS KKM
    - Borang Pendaftaran ID (Lampiran D) (jika berkaitan)
iii. Pegawai yang mengendalikan maklumat sensitif WAJIB menjalani tapisan keselamatan.
iv. Hak capaian diberikan berdasarkan prinsip ***Least Privilege***.
v. Tiada akses sistem aplikasi dibenarkan sebelum kelulusan lengkap.

8.3.1.2 Pegawai Bertukar Keluar / Tamat Perkhidmatan

i. Penolong Pegawai Aset Jabatan hendaklah memastikan pegawai memulangkan semua aset ICT.
ii. WAJIB melengkapkan Borang Pendaftaran ID (Lampiran D) dan diserahkan kepada UTMK. Semua akses sistem, e-mel dan fizikal yang berkenaan WAJIB ditamatkan serta-merta.

8.3.1.3 Peranan dan tanggungjawab pengguna adalah seperti berikut:

i. Membaca, memahami dan mematuhi Polisi ICT HTJS
ii. Menggunakan kemudahan ICT untuk urusan rasmi sahaja dan berkaitan tugas.
iii. Menjaga kerahsiaan ID pengguna dan kata laluan, serta tidak berkongsi dengan pihak lain.
iv. Menukar kata laluan secara berkala dan memastikan tahap keselamatan yang sesuai.

v. Melindungi maklumat pesakit dan data sulit hospital daripada akses tanpa kebenaran.

vi. Tidak memasang perisian atau aplikasi tanpa kebenaran UTMK.

vii. Tidak menyalahgunakan sistem ICT, termasuk akses tidak sah, muat turun bahan terlarang atau aktiviti menyalahi undang-undang.

viii. Melaporkan segera sebarang insiden keselamatan ICT seperti kehilangan data, virus, atau akses mencurigakan kepada UTMK.

ix. Menjaga peralatan ICT (komputer, pencetak, sistem rangkaian) yang digunakan daripada kerosakan atau penyalahgunaan.

x. Memastikan log keluar (log out) daripada sistem selepas selesai menggunakan komputer atau aplikasi.

xi. Mematuhi Polisi penggunaan e-mel dan internet rasmi yang ditetapkan oleh hospital.

xii. Bertanggungjawab ke atas semua aktiviti yang dilakukan menggunakan akaun ICT sendiri.

xiii. Melakukan salinan data/maklumat pada storan luar *(external hard disk)* untuk mengelakkan kehilangan data jika berlaku sebarang insiden.

xiv. Menghadiri program dan latihan mengenai ICT.

xv. Tidak memuat turun, membuat pemasangan dan menggunakan perisian yang boleh mendatangkan kemudaratan dan kerosakan kepada komputer dan rangkaian HTJS seperti perisian P2P *(peer to peer)*, perisian Proxy dan seumpamanya;

xvi. Bertanggungjawab ke atas semua peralatan dan perisian ICT termasuk penggunaan peralatan dan perisian ICT secara perkongsian (*sharing* dan *pool*);

xvii. Tidak mengguna atau mengambil tanpa kebenaran, menceroboh, mengubahsuai dan mencuri peralatan, perisian dan komponen ICT;

xviii. Tidak menggunakan peralatan ICT peribadi. Sekiranya amat diperlukan maka kerosakan dan kehilangan peralatan ICT peribadi adalah tanggungjawab pemilik.

xix. Tidak menggunakan aksesori atau komponen ICT hospital untuk kegunaan peralatan ICT peribadi.

9 PENGURUSAN POLISI ICT

9.1 Pelaksanaan Polisi

Pelaksanaan Polisi ini diarahkan oleh Pengarah HTJS dengan dibantu oleh perwakilan Jawatankuasa ICT (JICT) HTJS

9.2 Penyebaran Polisi

Polisi ini perlu disebarkan kepada semua pengguna dan dipertanggungjawabkan kepada UTMK

9.3 Semakan dan Pindaan Polisi

Polisi adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan arahan serta keperluan semasa. Berikut adalah prosedur berhubung dengan penyelenggaraan:

i. kenal pasti dan tentukan perubahan yang diperlukan;
ii. kemuka cadangan pindaan untuk persetujuan Mesyuarat JICT;
iii. perubahan yang telah dipersetujui oleh JICT dimaklumkan kepada semua pengguna; dan
iv. Polisi ini hendaklah dikaji semula sekurang-kurangnya sekali (1) setahun.

9.4 Pengecualian Polisi

Polisi adalah terpakai kepada semua pengguna dan tiada pengecualian diberikan kecuali atas izin CDO HTJS.

B BIDANG POLISI ICT

1 PENGURUSAN KESELAMATAN DIGITAL

1.1 PENGURUSAN KATA LALUAN

Perkara berikut perlu dipatuhi sebagai amalan terbaik dalam pengurusan kata laluan:

i. Kata laluan perlu mempunyai minima sekurang-kurangnya 12 aksara dengan gabungan huruf kecil, huruf besar, simbol dan nombor.
ii. Pengguna perlu menukar kata laluan selepas membuat capaian kali pertama ke dalam sistem aplikasi.
iii. Kata laluan hendaklah ditukar secara berkala dan tidak menggunakan kata laluan yang mudah diteka.
iv. Diwajibkan untuk menukar kata laluan selepas berlakunya insiden keselamatan.
v. Kata laluan terdahulu tidak boleh digunakan kembali.

1.2 KESELAMATAN MAKLUMAT

Pengguna bertanggungjawab memastikan keselamatan ID dan capaian sistem aplikasi yang diberikan. Sehubungan itu, perkara-perkara berikut hendaklah dipatuhi:

i. Pengguna tidak dibenarkan berkongsi ID dan kata laluan dengan mana-mana individu.
ii. Pengguna hendaklah menjaga kerahsiaan maklumat dan tidak mendedahkannya kepada pihak lain.
iii. Pengguna bertanggungjawab ke atas semua aktiviti yang dilaksanakan menggunakan ID masing-masing.

iv. Pengguna hendaklah segera memaklumkan kepada UTMK sekiranya terdapat sebarang aktiviti mencurigakan atau kemungkinan penyalahgunaan akaun.

v. Penggunaan ID hendaklah terhad kepada urusan rasmi sahaja.

vi. UTMK tidak bertanggungjawab ke atas sebarang kerosakan atau pencerobohan data atau sistem aplikasi jika kata laluan seseorang pengguna itu telah digunakan secara tidak sah oleh mereka yang tidak bertanggungjawab atas kelalaian pengguna itu sendiri.

1.3 TATACARA PENGURUSAN & PERLINDUNGAN REKOD ELEKTRONIK SEKTOR AWAM

Tujuan tatacara ini adalah bagi memastikan pengurusan rekod elektronik dilaksanakan secara teratur, selamat, dan mematuhi undang-undang bagi mengelakkan lima (5) risiko utama: pemalsuan, capaian tanpa kebenaran, penerbitan tanpa kebenaran, kehilangan, dan kemusnahan.

Tatacara Pelaksanaan:

i. Pengkategorian Rekod:
Semua rekod hendaklah dikategorikan mengikut tahap risiko keselamatan, tempoh pengekalan, dan jenis media. Ini termasuk (tetapi tidak terhad kepada) rekod peribadi/pesakit, rekod perundangan, rekod perakaunan, dan rekod transaksi perkhidmatan.

ii. Penyimpanan dan Rantaian Jagaan (*Chain of Custody*):
Rekod mestilah disimpan menggunakan proses dan sistem yang selamat bagi memelihara integriti serta mencegah manipulasi rekod. Penyimpanan mesti mematuhi Akta Arkib Negara 2003 [Akta 629], Arahan Keselamatan (Semakan dan Pindaan 2017) serta peraturan dan garis panduan berkaitan yang berkuat kuasa.

iii. Jadual Pengekalan Rekod:

Fasiliti mesti mengekalkan jadual penyimpanan rekod yang menetapkan tempoh simpanan yang wajib bagi setiap jenis rekod, selaras dengan tujuan perkhidmatan dan Polisi Arkib Negara.

iv. Pencapaian Semula (*Retrieval*):

Prosedur penyimpanan mesti memastikan rekod-rekod tersebut diurus dengan baik dan boleh diperoleh/dicapai semula dalam tempoh masa yang munasabah apabila diminta secara dalaman atau oleh pihak berkuasa.

v. Perlindungan Rekod Elektronik Jangka Panjang:

Rekod elektronik hendaklah dipelihara menggunakan kaedah yang sesuai bagi memastikan ia kekal boleh diakses, dibaca, digunakan dan disahkan ketulenannya sepanjang tempoh penyimpanan, walaupun berlaku perubahan teknologi. Ini termasuk penggunaan format fail yang standard, penyimpanan metadata dan maklumat kriptografi yang berkaitan, serta pelaksanaan migrasi format apabila diperlukan.

vi. Pelupusan Rekod Selamat:

Sebaik sahaja tempoh pengekalan sesuatu rekod tamat dan mendapat kelulusan pelupusan, ia mestilah dimusnahkan secara selamat. Peralatan digital yang mengandungi rekod mesti dimusnahkan secara fizikal atau dipadam secara kekal bagi menghalang pembocoran data.

1.4 TATACARA KESELAMATAN MAKLUMAT DALAM HUBUNGAN PIHAK KETIGA

Tujuan tatacara ini adalah bagi memastikan semua penglibatan pihak ketiga dikawal secara selamat bagi melindungi aset dan maklumat HTJS.

1.4.1 Pematuhan Kontrak

i. Semua kontrak, SLA atau perjanjian lain yang melibatkan pihak ketiga hendaklah memasukkan keperluan keselamatan ICT, perlindungan maklumat, pematuhan perundangan serta tanggungjawab pihak-pihak yang terlibat.

ii. Pihak ketiga hendaklah menandatangani dokumen yang berkaitan sebelum diberi akses kepada aset atau maklumat ICT, termasuk tetapi tidak terhad kepada:

- Surat Akuan Pematuhan PKS KKM;
- Surat Akuan di bawah Akta Rahsia Rasmi 1972 [Akta 88]; dan
- Perjanjian Kerahsiaan (*Non-Disclosure Agreement* (NDA)), jika berkaitan.

1.4.2 Tapisan Keselamatan

Semua kakitangan kontraktor yang terlibat dengan projek di HTJS WAJIB melalui e-Vetting Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) sebelum akses diberikan.

1.4.3 Kawalan Capaian

i. Akses diberikan berdasarkan keperluan sahaja.

ii. Semua aktiviti kontraktor mesti dipantau.

iii. Akses adalah sementara dan boleh ditarik balik bila-bila masa.

1.4.4 Kawalan Penyelenggaraan

i. Kontraktor WAJIB diiringi pegawai HTJS sepanjang masa.

ii. Kontraktor WAJIB memakai tag pengenalan diri yang dibekalkan oleh Unit Keselamatan HTJS.

1.4.5 Penamatan Kontrak

i. ID kontraktor hendaklah ditamatkan.

ii. Semua data mesti dipulangkan / dihapuskan.

iii. Pihak kontraktor tidak dibenarkan mengakses sistem aplikasi, server, pangkalan data dan lain-lain yang berkaitan setelah tamat tempoh kontrak.

1.5 TATACARA PELAPORAN DAN LOG INSIDEN KESELAMATAN SIBER HTJS

Tujuan tatacara ini adalah bagi menyediakan mekanisme pelaporan dan tindak balas insiden keselamatan siber secara cepat dan berkesan.

1.5.1 Tatacara ini terpakai semua insiden keselamatan seperti:

i. Virus / Malware
ii. *Data breach*
iii. *Unauthorized access*
iv. Bencana

1.5.2 Pelaporan

i. Pengguna hendaklah melaporkan insiden kepada ICTSO dengan segera.
ii. ICTSO hendaklah melaporkan insiden kepada *Computer Security Incident Response Team* (CSIRT) KKM.

1.5.3 Penilaian Insiden

CSIRT akan menentukan tahap sama ada Rendah / Sederhana / Tinggi / Kritikal.

1.5.4 Pengumpulan Bukti

i. Log sistem dikumpul
ii. *Chain of custody* dijaga

1.5.5 Tindakan

i. Pemulihan sistem
ii. Makluman laporan pemulihan ke CSIRT KKM

1.5.6 *Post-Mortem*

i. *Root cause analysis*

ii. Cadangan penambahbaikan

1.6 TATACARA PENGGUNAAN INTERNET

1.6.1 Pengguna yang melayari internet adalah bertanggungjawab sepenuhnya ke atas maklumat yang dikunci masuk serta capaian yang dilakukan.

1.6.2 Pengguna tidak dibenarkan menggunakan modem untuk membuat capaian terus ke internet TANPA kebenaran daripada UTMK.

1.6.3 Penggunaan *Internet Proxy* untuk capaian ke internet adalah dilarang.

1.6.4 Penghantaran dan penerimaan dokumen yang mengandungi maklumat rahsia rasmi melalui internet tidak dibenarkan sama sekali tanpa perisian penyulitan (*encryption*) yang dibenarkan.

1.6.5 Pengguna tidak dibenarkan membuat capaian kepada bahan-bahan terlarang dengan menggunakan kemudahan pejabat. Ini termasuk capaian laman yang berbentuk hiburan, lucah dan perjudian.

1.6.6 Pengguna dilarang menggunakan capaian yang membebankan rangkaian seperti radio *online*, video *streaming* dan permainan komputer *online*.

1.6.7 Pengguna adalah dilarang daripada melayari laman-laman web yang tidak berkaitan dengan tugas rasmi semasa waktu pejabat termasuk media sosial seperti Facebook, Instagram, X dan lain-lain platform seumpamanya.

1.6.8 Pentadbir Keselamatan berhak menapis, menghalang dan mencegah penggunaan mana-mana laman web yang tidak sesuai.

1.6.9 Pentadbir Keselamatan diberi kuasa untuk menyediakan laporan penggunaan capaian rangkaian dan internet HTJS kepada pihak pengurusan jika diperlukan.

1.7 TATACARA KAWALAN CAPAIAN HTJS

Tatacara ini bertujuan menetapkan kawalan yang ketat ke atas pemberian, pengurusan, dan pembatalan hak capaian ke atas sistem aplikasi, rangkaian, dan data bagi meminimumkan risiko capaian tanpa kebenaran, pencerobohan, atau kebocoran maklumat.

Prosedur Pelaksanaan:

i. Prinsip Asas Capaian:
Capaian kepada sistem aplikasi dan maklumat hanya diberikan berdasarkan prinsip "Perlu Mengetahui" (*Need-to-Know*) dan "Hak Capaian Minimum" (*Least Privilege*). Pengguna hanya diberi fungsi capaian (membaca, menulis, menghapus, melaksana) yang sekadar cukup untuk menjalankan tugas rasmi mereka.

ii. Pengurusan Identiti Pengguna:
Setiap pengguna mesti diberikan satu identiti (ID) pengesahan yang unik. Pengguna dilarang sama sekali berkongsi maklumat log masuk (kata laluan) atau membenarkan pihak lain menggunakan ID mereka.

iii. Kebenaran dan Kelulusan Capaian:
Pemberian hak capaian mestilah melalui proses permohonan yang formal dan memerlukan sekurang-kurangnya dua tahap kelulusan berbeza (contoh: sokongan penyelia dan kelulusan pemilik sistem aplikasi).

iv. Semakan Hak Capaian Berkala:

Hak capaian semua pengguna mesti disemak, dikemas kini, dan disahkan secara berkala, sekurang-kurangnya setahun sekali. Semakan lebih kerap diperlukan bagi pengguna yang memegang "Hak Capaian Istimewa" (*Administrator / Superuser*).

v. Pembatalan Capaian (Serta-Merta):

Capaian sistem aplikasi dan fizikal mesti dibatalkan atau ditarik balik dengan segera sekiranya pengguna (pegawai atau pihak ketiga) tamat perkhidmatan, bersara, ditamatkan kontrak, bertukar jabatan, bercuti panjang (melebihi 3 bulan), atau sedang dalam siasatan tatatertib.

vi. Pengurusan Capaian Dinamik:

Bagi meningkatkan keselamatan, sistem kawalan capaian boleh disesuaikan secara dinamik berdasarkan konteks. Sebagai contoh, hak capaian pengguna boleh dihadkan jika cuba mencapai sistem aplikasi di luar waktu pejabat atau dari lokasi yang tidak dikenali

2 PENGURUSAN PUSAT DATA

2.1 Pentadbir pusat data adalah bertanggungjawab kepada perkara-perkara berikut:

i. Mengawal dan mengurus setiap aktiviti yang berlaku di dalam pusat data dan memastikan pusat data bebas daripada aktiviti sabotaj, kecurian dan jenayah melalui sistem pemantauan yang berterusan;

ii. Memantau dan merekod maklumat personel yang keluar dan masuk ke pusat data melalui sistem akses dan merekodkan semua pergerakan keluar / masuk Bilik Server dalam Buku Log Keluar / Masuk Pusat Data;

iii. 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

iv. Sentiasa menjaga kebersihan dan kekemasan pusat data supaya tidak terdedah kepada habuk dan memastikan tidak menyimpan atau menempatkan peralatan yang tidak diperlukan.

2.2 TATACARA PENGURUSAN PUSAT DATA

2.2.1 Kawalan capaian ke pusat data perlulah mempunyai ciri-ciri keselamatan seperti penggunaan sistem kad akses atau kata laluan.

2.2.2 Kebenaran masuk ke kawasan persekitaran pusat data hendaklah diiringi oleh sekurang-kurangnya seorang pentadbir sistem aplikasi atau kakitangan teknikal UTMK yang dilantik bagi menentukan dan mengawal selia tugasan yang diperlukan.

2.2.3 Aktiviti yang dilaksanakan oleh pentadbir sistem aplikasi atau pembekal hendaklah direkodkan ke dalam Buku Log Keluar / Masuk Pusat Data yang disediakan.

2.2.4 Sebarang pemindahan maklumat daripada pusat data hendaklah dipohon dan mendapat kebenaran daripada pemilik data (*data owner*), pentadbir sistem aplikasi masing-masing atau Ketua UTMK melalui saluran rasmi.

2.2.5 Pusat data hendaklah mempunyai sistem pengudaraan *(ventilation)* yang mencukupi dan alat pendingin hawa yang berupaya mengawal kelembapan udara dengan julat 20-30 RH dan suhu antara 18-25°C. Suhu dan kelembapan harian akan direkodkan.

2.2.6 Pusat data mesti dilengkapi dengan media CCTV untuk memudahkan pemantauan dilakukan.

2.2.7 Pegawai bertanggungjawab perlu memastikan peralatan ICT berfungsi dengan baik jika terdapat sebarang gangguan dalam bilik server.

2.3 TATACARA PENGURUSAN *SERVER*

2.3.1 Kunci rak-rak *server* perlu disimpan di dalam peti kunci yang berkunci di dalam bilik Penyelia.

2.3.2 Penyelenggaraan fizikal semua *server* perlu dilaksanakan sekurang-kurangnya dua (2) kali setahun.

2.3.3 Setiap *server* perlu dipasang perisian *antivirus* berlesen.

2.3.4 Pengurusan kata laluan bagi setiap *server* hendaklah merujuk perkara D(1)(1.1) dalam polisi ini iaitu Pengurusan Kata Laluan di bawah tajuk Keselamatan Digital & Pusat Data.

2.3.5 Jika pembekal memerlukan akses secara *remote* ke atas sistem aplikasi utama bagi kes-kes kritikal (*unplanned*), pembekal perlu membuat permohonan rasmi kepada UTMK.

2.4 TATACARA *BACKUP* DAN *RESTORE*

2.4.1 Kekerapan pelaksanaan *backup* data / maklumat yang dilakukan adalah *Backup* Harian, *Backup* Mingguan, *Backup* Bulanan dan mengikut keperluan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

i. Membuat *backup* ke atas sistem aplikasi dan pangkalan data;

ii. Menguji *backup* sedia ada dengan melaksanakan aktiviti *restore* sekurang-kurangnya sekali (1) setahun bagi memastikan sistem aplikasi / data dapat berfungsi dengan sempurna.

2.4.2 Bagi memastikan kesinambungan perkhidmatan ICT dan pemulihan data sekiranya berlaku bencana, salinan backup hendaklah disimpan di lokasi *off-site* yang telah ditetapkan, iaitu di Hospital Rembau. Pelaksanaan *backup off-site* hendaklah mematuhi perkara-perkara berikut:

i. Salinan *backup* hendaklah direplikasi atau dipindahkan daripada pusat data Hospital Tuanku Ja'afar Seremban (HTJS) ke lokasi *off-site* di Hospital Rembau mengikut jadual yang telah ditetapkan.

ii. Data *backup* hendaklah disimpan dalam persekitaran yang selamat serta dilindungi daripada risiko kehilangan, kerosakan, bencana alam, akses tanpa kebenaran dan ancaman keselamatan siber.

iii. Semua data yang dipindahkan ke lokasi *off-site* hendaklah menggunakan mekanisme penyulitan (*encryption*) dan saluran komunikasi yang selamat bagi memastikan kerahsiaan serta integriti data.

iv. Akses kepada sistem dan media *backup off-site* hendaklah dihadkan kepada pegawai yang diberi kuasa sahaja serta direkodkan untuk tujuan pemantauan dan audit.

v. Pengujian *restore* daripada salinan backup *off-site* hendaklah dilaksanakan sekurang-kurangnya sekali (1) setahun atau selepas sebarang perubahan besar kepada sistem bagi memastikan data dapat dipulihkan dengan lengkap dan perkhidmatan dapat diteruskan dalam tempoh yang ditetapkan.

vi. Tempoh penyimpanan salinan *backup* hendaklah mematuhi polisi pengurusan rekod, keperluan operasi serta dasar keselamatan ICT KKM yang sedang berkuat kuasa.

vii. Semua aktiviti *backup*, replikasi, pemindahan, penyimpanan dan *restore* hendaklah direkodkan serta dipantau secara berkala bagi memastikan keberkesanan pelan pemulihan bencana (*Disaster Recovery Plan* - DRP) dan PKP hospital.

3 PENGURUSAN MEJA BANTUAN (*HELPDESK*) ICT

3.1 Objektif meja bantuan ICT adalah menyediakan perkhidmatan bantuan peringkat pertama (*1st tier*) kepada pengguna yang bertugas di hospital. Matlamat utama adalah memastikan kelangsungan operasi perkhidmatan ICT organisasi dengan menyediakan sokongan teknikal yang cekap, pantas, dan berkesan kepada pengguna.

3.2 Skop perkhidmatan meja bantuan ICT meliputi pengendalian aduan, permintaan perkhidmatan *(service request)*, pertanyaan pengguna, serta penyaluran maklumat gangguan perkhidmatan.

3.3 Meja bantuan ICT beroperasi hanya pada waktu pejabat dan boleh dihubungi melalui sambungan 4275. Selepas waktu pejabat atau cuti umum, aduan ICT perlu melalui operator hospital dan akan disambungkan kepada kontraktor / pegawai *on-call* UTMK yang bertugas.

3.4 TATACARA PENGURUSAN ADUAN

3.4.1 Penerimaan dan Perekodan Aduan

i. Kakitangan UTMK menerima aduan atau permohonan melalui e-mel, panggilan telefon atau pengguna hadir secara terus (*walk-in*).
ii. Maklumat aduan didaftarkan ke dalam Sistem Aduan ICT. Butiran wajib termasuk nama, lokasi, nombor telefon pelapor, jenis aduan, serta masalah dan tahap kerosakan.

3.4.2 Pengagihan Aduan

i. Aduan yang direkodkan akan diagihkan kepada kakitangan UTMK yang berkaitan untuk tindakan lanjut.
ii. Kakitangan yang ditugaskan hendaklah menerima agihan tugas dan mengenal pasti sama ada peralatan tersebut berada di bawah kontrak

penyelenggaraan, kontrak penyewaan atau tidak tertakluk kepada mana-mana kontrak.

3.4.3 Tindakan Penyelenggaraan dan Pembaikan

i. Peralatan di bawah kontrak penyelenggaraan / penyewaan / dalam tempoh jaminan

Kerosakan dilaporkan kepada kontraktor yang terlibat dan pemantauan dilakukan sehingga pembaikan diselesaikan oleh kontraktor mengikut SLA dalam dokumen perjanjian.

ii. Peralatan tidak tertakluk kepada mana-mana kontrak

Semua peralatan yang tidak tertakluk kepada mana-mana kontrak adalah di bawah seliaan UTMK.

- **Tindakan Teknikal:** Kakitangan UTMK akan melaksanakan pembaikan secara dalaman atau menggunakan alat ganti sedia ada.
- **Perolehan Luar:** Sekiranya memerlukan kepakaran luar, proses perolehan akan dilaksanakan oleh UTMK tertakluk kepada kelulusan pengarah hospital.

3.4.4 Penutupan Aduan

Pegawai UTMK perlu menyemak aduan dan mengesahkan status penyelesaian pembaikan sebelum menutup aduan tersebut.

3.4.5 Segala aduan, maklumat penyelenggaraan dan penyelesaian masalah hendaklah direkodkan di dalam Sistem Aduan ICT.

4 KHIDMAT SOKONGAN TEKNIKAL ICT

4.1 TATACARA PENGURUSAN KHIDMAT SOKONGAN TEKNIKAL ICT

4.1.1 Khidmat Sokongan Peralatan ICT

i. Sokongan Peralatan ICT merangkumi aktiviti pemasangan, konfigurasi, penyelenggaraan dan pembaikan peralatan ICT bagi memastikan semua peralatan berada dalam keadaan baik, berfungsi dengan sempurna dan dapat menyokong operasi organisasi secara berterusan.

ii. Peralatan yang terlibat termasuk komputer peribadi, komputer riba, pencetak, pengimbas, peralatan persidangan video serta peralatan ICT lain yang digunakan oleh pengguna.

iii. UTMK hendaklah menjalankan pemeriksaan terhadap peralatan ICT yang mengalami kerosakan atau gangguan fungsi bagi mengenal pasti punca masalah. Tindakan pembaikan, penggantian komponen atau penyelenggaraan yang bersesuaian hendaklah dilaksanakan mengikut keperluan.

iv. Sekiranya peralatan ICT memerlukan pemeriksaan lanjut atau penggantian alat ganti yang tidak dapat dilaksanakan di lokasi pengguna, pengguna hendaklah menghantar peralatan tersebut ke Pejabat Teknikal ICT untuk tujuan pembaikan. Setelah kerja-kerja pembaikan selesai, pengguna bertanggungjawab mengambil semula peralatan ICT tersebut di Pejabat Teknikal.

v. Setelah tindakan diambil, peralatan hendaklah diuji bagi memastikan ia kembali berfungsi dengan baik sebelum diserahkan semula kepada pengguna.

vi. Semua aktiviti penyelenggaraan dan pembaikan hendaklah direkodkan untuk tujuan pemantauan dan rujukan.

4.1.2 Khidmat Sokongan Perisian

i. Sokongan perisian melibatkan pengurusan sistem operasi dan perisian yang digunakan dalam HTJS bagi memastikan ia dapat beroperasi dengan stabil, selamat dan memenuhi keperluan pengguna.

ii. Skop ini merangkumi pemasangan, konfigurasi, pengemaskinian, penyelenggaraan dan penyelesaian masalah yang berkaitan dengan perisian.
iii. UTMK hendaklah memastikan sistem operasi dan perisian yang digunakan sentiasa dikemaskini mengikut keperluan semasa serta mematuhi keperluan keselamatan ICT HTJS.
iv. Sebarang masalah berkaitan kegagalan perisian, ralat perisian atau gangguan fungsi hendaklah dianalisis dan tindakan pembetulan yang sesuai hendaklah dilaksanakan.
v. Pengujian hendaklah dilakukan selepas kerja penyelenggaraan atau pembaikan bagi memastikan perisian dapat digunakan dengan baik tanpa menjejaskan operasi pengguna.

4.1.3 Khidmat Sokongan Rangkaian ICT

i. Sokongan Rangkaian ICT bertujuan memastikan perkhidmatan rangkaian sentiasa tersedia, stabil dan mampu menyokong keperluan operasi organisasi.
ii. Skop ini merangkumi penyelenggaraan rangkaian setempat (LAN), rangkaian tanpa wayar (WiFi), sambungan internet, peralatan rangkaian dan komponen berkaitan.
iii. UTMK hendaklah memantau dan menyemak status rangkaian secara berkala bagi memastikan semua peralatan dan sambungan rangkaian berfungsi dengan baik.
iv. Sebarang gangguan rangkaian hendaklah disiasat bagi mengenal pasti punca masalah sebelum tindakan pembetulan dilaksanakan.
v. Aktiviti konfigurasi, penyelenggaraan dan pengoptimuman rangkaian hendaklah dilaksanakan mengikut keperluan bagi memastikan prestasi rangkaian berada pada tahap yang optimum.
vi. Pengujian sambungan hendaklah dilakukan selepas setiap kerja penyelenggaraan atau konfigurasi bagi memastikan perkhidmatan rangkaian dapat digunakan seperti yang ditetapkan.

4.1.4 Khidmat Sokongan Infrastruktur ICT

i. Sokongan infrastruktur ICT melibatkan pengurusan dan penyelenggaraan kemudahan fizikal yang menyokong operasi sistem dan perkhidmatan ICT HTJS.

ii. Infrastruktur yang terlibat termasuk Telecommunication Room (TCR), rak peralatan ICT, sistem bekalan kuasa tanpa gangguan (UPS), sistem pendawaian berstruktur, patch panel dan kemudahan sokongan ICT yang berkaitan.

iii. Kakitangan ICT hendaklah melaksanakan pemeriksaan berkala bagi memastikan infrastruktur ICT berada dalam keadaan teratur, selamat dan berfungsi dengan baik.

iv. Sebarang kerosakan, ketidakpatuhan atau risiko yang boleh menjejaskan operasi ICT hendaklah dikenal pasti dan tindakan pembetulan hendaklah diambil dengan segera.

4.1.5 Keadaan persekitaran seperti bekalan kuasa, kebersihan dan susunan peralatan juga hendaklah dipantau bagi memastikan ia memenuhi keperluan operasi dan keselamatan ICT HTJS.

5 PENGURUSAN RANGKAIAN

5.1 Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut:

i. Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di HTJS beroperasi sepanjang masa

ii. Memastikan semua peralatan dan perisian rangkaian diselenggara dengan sempurna

iii. Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada

iv. Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil

v. 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

vi. Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian

vii. Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian

5.2 Kemudahan rangkaian hanya boleh digunapakai oleh pengguna bagi tujuan rasmi.

5.3 Pengguna tidak boleh mengguna rangkaian di HTJS untuk aktiviti-aktiviti yang bertentangan dengan undang-undang atau peraturan-peraturan KKM, negeri dan negara. Ini termasuk menghantar dan menerima maklumat yang berunsur subversif.

5.4 UTMK bertanggungjawab menyelenggara rangkaian setempat, talian internet dan perkhidmatan talian Kerajaan yang diberi melalui Projek MyGovNet.

5.5 Peralatan rangkaian di HTJS merangkumi peralatan seperti berikut:

i. *Firewall*
ii. *Switches*
iii. *Server*
iv. *Router*
v. *Node* rangkaian
vi. *Wireless Access Point*
vii. *Infrastruktur* kabel rangkaian
viii. *Network Rack*

5.6 Semua peralatan rangkaian hendaklah diletakkan di tempat yang dikhaskan seperti di bilik server / bilik TCR / rak. Sebarang perubahan lokasi peralatan rangkaian perlu mendapatkan kelulusan UTMK.

5.7 Sebarang penyambungan rangkaian tambahan perlu mendapat kebenaran dan dimaklumkan terlebih dahulu kepada UTMK dan mematuhi piawaian yang ditetapkan.

5.8 Semua pengguna yang menggunakan peralatan ICT peribadi perlu merujuk kepada UTMK serta dilengkapi dengan perisian *antivirus* yang terkini sebelum dibenarkan akses ke rangkaian HTJS. Sebarang kerosakan dan serangan virus ke atas peralatan ICT peribadi adalah di bawah tanggungjawab pengguna.

5.9 Pengguna tidak boleh membuat tambahan nod rangkaian (berwayar atau tanpa wayar) tanpa mendapat kelulusan UTMK.

5.10 Pemasangan *wireless access point* (WAP) peribadi adalah tidak dibenarkan bagi mengelakkan sebarang gangguan terhadap rangkaian sedia ada kecuali atas justifikasi yang kukuh. Pihak UTMK berhak untuk menanggalkan pemasangan WAP yang dipasang tanpa kebenaran UTMK.

5.11 TCR hanya menempatkan peralatan ICT dan peralatan lain dengan kebenaran UTMK.

5.12 Semua kabel rangkaian hendaklah dipasang dengan kemas seperti di bawah lantai atau melalui *conduit*, yang mana bersesuaian.

5.13 Semua trafik keluar dan masuk hendaklah melalui satu *gateway* sahaja iaitu *firewall* yang dikawal oleh UTMK.

5.14 Sebarang perisian yang boleh menceroboh keselamatan rangkaian dan komunikasi tidak dibenarkan penggunaannya sama sekali melainkan mendapat kelulusan UTMK.

5.15 Penyediaan Infrastruktur Rangkaian Bangunan Baharu / Ubahsuai Bangunan hendaklah dimaklumkan kepada UTMK melalui saluran rasmi dan perlu memasukkan keperluan infrastruktur rangkaian dengan mengambil kira:

i. Pemasangan kabel rangkaian perlu menggunakan PVC *conduit / trunking* dan dilabel;
ii. Pemasangan kabel mestilah disambung ke rak switch yang berhampiran; dan
iii. Jika melibatkan perolehan peralatan rangkaian, peralatan tersebut perlu mempunyai ciri-ciri menyokong IPV4 dan IPV6 *Compliance (Dual Stack)*.

6 PENGURUSAN ASET ICT

6.1 TATACARA PEROLEHAN PERALATAN DAN PERISIAN ICT

6.1.1 Proses perolehan Peralatan dan Perisian ICT hendaklah mendapatkan kelulusan teknikal dengan merujuk kepada pekeliling terpakai sedia ada iaitu Surat Pekeliling Am Bilangan 7 Tahun 2024 Garis Panduan Permohonan Kelulusan Teknikal Dan Pemantauan Projek Teknologi Maklumat Dan Komunikasi (ICT) Sektor Awam serta Pekeliling Perbendaharaan yang sedang berkuatkuasa.

6.1.2 Sebarang perolehan ICT yang dilakukan melalui jabatan / unit di HTJS perlu mempunyai dokumen lengkap dan melaksanakan pengujian dan pentauliahan peralatan bersama UTMK dan Unit Pengurusan Aset dan Stor sebelum pendaftaran dilakukan di dalam Sistem Pemantauan Pengurusan Aset (SPPA).

6.1.3 Semua peralatan dan perisian ICT tidak dibenarkan dijual, disewa, dipaten, dipinjam, disebar atau diberi kepada sesiapa tanpa kebenaran UTMK HTJS.

6.1.4 Sumbangan peralatan ICT perlu didaftarkan sebagai aset kerajaan untuk memudahkan penyelenggaraan dan pembekalan consumable item. Pihak jabatan/unit yang menerima sumbangan peralatan ICT mestilah memaklumkan

kepada Unit Pengurusan Aset & Stor dan hendaklah mematuhi Tatacara Pengurusan Aset Alih Kerajaan (TPA) 1 Pekeliling Perbendaharaan (1PP) fasal AM 2.3/2013 atau pekeliling yang sedang berkuatkuasa.

6.2 TATACARA AGIHAN PERALATAN ICT

6.2.1 Agihan komputer, laptop dan mesin pencetak dilaksanakan berdasarkan kepada keperluan dan stok semasa.

6.2.2 Penyerahan peralatan ICT perlu disertakan dengan Borang Pengesahan ICT (Lampiran D).

6.2.3 Peralatan dan perisian ICT yang telah diagihkan kepada pengguna tidak digalakkan berpindah milik atau lokasi sepertimana yang telah ditetapkan dan tercatat di dalam borang Kew.PA-7 (Senarai Aset Alih Kerajaan).

6.2.4 Sebarang pemindahan peralatan ICT perlu dimaklumkan kepada UTMK.

6.2.5 Pengguna perlu bertanggungjawab ke atas peralatan ICT yang digunakan secara gunasama.

6.2.6 Sekiranya pengguna bertukar secara dalaman atau keluar dari HTJS, pengguna atau penyelia jabatan / unit hendaklah mematuhi Tatacara Pengurusan Aset Alih Kerajaan (TPA) 1 Pekeliling Perbendaharaan (1PP) fasal AM 2.3/2013 dan memaklumkan secara rasmi kepada UTMK bagi memastikan nama pengguna tersebut dikeluarkan daripada senarai peralatan dan peralatan ICT yang dipertanggungjawabkan.

6.3 TATACARA PENGGUNAAN PERALATAN ICT

6.3.1 Semua peralatan ICT yang telah dibekalkan adalah hakmilik HTJS dan hendaklah digunakan untuk urusan rasmi sahaja.

6.3.2 Kakitangan yang telah dibekalkan peralatan ICT bertanggungjawab untuk:

i. memastikan peralatan ICT disimpan dengan selamat;

ii. digunakan dengan baik mengikut peraturan norma penggunaan peralatan;

iii. melaporkan sebarang kerosakan kepada UTMK; dan

iv. melaporkan sebarang kehilangan kepada Unit Pengurusan Aset dan Stor serta.

6.3.3 Sebarang perpindahan peralatan ICT hendaklah dimaklumkan kepada UTMK.

6.3.4 Pergerakan peralatan ICT gunasama di jabatan / unit hendaklah menggunakan Borang Permohonan Pergerakan / Pinjaman Aset Alih (Kew.PA-9).

6.3.5 Pengguna tidak dibenarkan memasang mana-mana perisian / program ke dalam komputer / komputer riba yang dibekalkan. Sebarang pemasangan perisian / program yang diperlukan akan dilakukan oleh UTMK.

6.3.6 UTMK tidak bertanggungjawab atas kerosakan / kehilangan data dalam media storan pengguna seperti hard disk, external hard disk, thumb drive dan lain-lain. Pengguna adalah bertanggungjawab sepenuhnya atas keselamatan data tersebut.

6.3.7 Pengurusan kata laluan *administrator* bagi setiap komputer peribadi dan komputer riba di HTJS adalah di bawah pengendalian UTMK.

6.4 TATACARA PENYELENGGARAAN PERALATAN ICT

6.4.1 Bantuan teknikal / aduan tentang masalah-masalah yang dihadapi dalam penggunaan ICT perlu diajukan kepada UTMK.

6.4.2 Memastikan pengasingan akaun Administrator dan Pengguna pada komputer atau komputer riba yang dibekalkan.

6.4.3 Peralatan ICT yang ingin dibaikpulih perlu dibawa sendiri ke pejabat teknikal ICT.

6.4.4 Pengguna mesti memastikan storage device (external hard disk, CD/DVD atau *thumbdrive*) yang menyimpan dokumen terhad disimpan di tempat yang selamat;

6.4.5 Berikut adalah jadual tempoh masa yang diperlukan bagi penyelenggaraan tidak berjadual bagi peralatan ICT:

Bil.	Perkara	Tempoh
1.	Penyelenggaran peralatan ICT yang tidak melibatkan alat ganti atau pemasangan perisian	6 jam
2.	Penyelenggaran peralatan ICT memerlukan pemasangan semula (*reformat*) dan tidak melibatkan alat ganti	3 hari bekerja. Tertakluk kepada keadaan semasa.
3.	Penyelenggaran peralatan ICT yang melibatkan pemasangan serta melibatkan alat ganti dan perlu dibuat perolehan Kerosakan yang melibatkan penggantian: a) dalam waranti b) tanpa waranti	30 hari bekerja. Tertakluk kepada keadaan semasa.
4.	Penyelenggaran peralatan ICT di bawah kontrak KKM.	Tertakluk kepada jadual penyelenggaraan kontrak projek.

6.4.6 Semua kerosakan peralatan ICT yang di bawah kawal selia UTMK dan melibatkan kos perlu mengisi Borang Permohonan Pergerakan / Pinjaman Aset Alih (Kew.PA-9) pada Sistem Pengurusan Aset bagi mendapatkan kelulusan penyenggaraan peralatan tersebut.

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

6.5 TATACARA PERMOHONAN PERALATAN DAN PERISIAN ICT BAHARU

6.5.1 Pengguna perlu mengemukakan permohonan peralatan atau perisian ICT beserta justifikasi secara rasmi kepada UTMK.

6.5.2 Sebarang pengagihan peralatan atau perisian ICT akan disertakan dengan Borang Pengesahan ICT (Lampiran D) dan memo / e-mel.

6.6 TATACARA PEMINJAMAN PERALATAN DAN PERISIAN ICT

6.6.1 UTMK menyediakan kemudahan pinjaman peralatan ICT bagi tujuan urusan rasmi sahaja.

6.6.2 Permohonan mestilah dibuat sekurang-kurangnya tiga (3) hari bekerja sebelum tarikh peminjaman melalui surat / memo urusan rasmi tersebut.

6.6.3 Pihak UTMK akan memproses permohonan pinjaman mengikut jumlah peralatan ICT yang tersedia pada masa tersebut.

6.6.4 Peminjaman peralatan ICT dari agensi luar perlu mendapat kelulusan Pengarah HTJS.

6.6.5 Tempoh maksimum pinjaman peralatan adalah selama tujuh (7) hari bekerja. Peminjam dikehendaki mengisi Borang Permohonan Pergerakan / Pinjaman Aset Alih (Kew.PA-9) semula untuk melanjutkan tempoh pinjaman.

6.6.6 Bagi peminjaman untuk kegunaan rasmi semasa waktu pejabat, peminjam atau wakil hendaklah hadir sendiri untuk mengambil, mengisi borang dan memulangkan peralatan tersebut daripada / kepada pihak UTMK.

6.6.7 Peminjam perlu memaklumkan kepada pihak UTMK 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.

6.6.8 Pengguna tidak dibenarkan membuat pengubahsuaian kepada peralatan dan perisian ICT. Peminjam bertanggungjawab ke atas keselamatan, kerosakan dan kehilangan peralatan ICT tersebut.

6.6.9 Peminjam dikehendaki memulangkan semula peralatan yang dipinjam mengikut tarikh pinjaman. Semua peralatan yang dipinjam mestilah dipulangkan dalam waktu pejabat.

6.6.10 Pihak UTMK 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.

6.6.11 Bagi pinjaman komputer riba, pengguna dari jabatan / unit yang telah dibekalkan kemudahan komputer riba perlu menggunakan komputer riba jabatan / unit tersebut.

6.6.12 Sekiranya berlaku kehilangan, peminjam perlu merujuk kepada pihak Unit Pengurusan Aset dan Stor untuk tindakan berdasarkan Tatacara Pengurusan Aset Alih Kerajaan.

6.6.13 Pengurusan logistik peralatan ICT adalah di bawah tanggungjawab peminjam.

6.6.14 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 UTMK tidak bertanggungjawab ke atas kehilangan atau penyalahgunaan data / fail peminjam yang di simpan dalam peralatan ICT

yang dipinjamkan. Pihak UTMK akan memadam data / fail tersebut selepas peralatan ICT dipulangkan semula.

6.7 TATACARA PELUPUSAN PERALATAN DAN PERISIAN ICT

Semua peralatan yang didapati tidak sesuai dinaiktaraf atau diselenggara, dilupus mengikut Tatacara Pengurusan Aset Alih (1PP).

6.7.1 TATACARA PELUPUSAN MEDIA STORAN

Tujuan tatacara ini adalah bagi memastikan kerahsiaan maklumat terpelihara serta mengelakkan sebarang kebocoran atau kehilangan kawalan terhadap maklumat tersebut melibatkan media storan (seperti *hard disk, pendrive*, pelayan) yang dilupuskan atau diguna semula.

Prosedur Pelaksanaan:

i. Pembersihan Data (Sanitasi): Sebelum pelupusan atau penggunaan semula, peralatan yang mempunyai peranti media storan mestilah diperiksa. Maklumat sensitif yang disimpan padanya hendaklah dipadamkan, diformat semula, atau ditulis ganti *(overwrite)* secara kekal. Ia hendaklah disanitasi secara logikal mahupun fizikal.
ii. Pemusnahan Fizikal: Bagi media storan yang menyimpan maklumat sensitif dan tidak lagi diperlukan, pemusnahan terkawal secara fizikal adalah wajib dilakukan.
iii. Penglibatan Pihak Ketiga: Jika fasiliti menggunakan pihak ketiga untuk mengumpul dan melupuskan media storan, pemilihan mestilah dibuat secara teliti bagi memastikan mereka cekap dan mempunyai kawalan yang sewajarnya.
iv. Jejak Audit: Segala proses pelupusan media storan mestilah didokumentasikan dengan lengkap untuk tujuan jejak audit.

6.8 TATACARA PENGGUNAAN *BRING YOUR OWN DEVICE* (BYOD)

Tujuan tatacara ini adalah bagi menetapkan kawalan keselamatan untuk membenarkan pengguna menggunakan peralatan peribadi (seperti komputer riba atau telefon pintar) untuk mengakses sistem aplikasi dan data rasmi organisasi.

Pengguna BYOD perlu mematuhi tatacara penggunaan BYOD seperti berikut:

i. Semua peringkat maklumat rasmi kerajaan adalah hakmilik kerajaan;

ii. Sebarang bahan rasmi yang dimuatnaik/ edar/ kongsi hendaklah mendapat kebenaran Ketua Jabatan;

iii. Menandatangani Surat Akuan Pematuhan Polisi ICT, Surat Akuan Pematuhan PKS KKM dan Akta Rahsia Rasmi 1972 [Akta 88];

iv. Memastikan peranti yang digunakan mempunyai kawalan keselamatan standard seperti kata laluan, antivirus, patching terkini dan anti theft.

v. Pengguna adalah dilarang daripada melakukan perkara berikut:

- Menyimpan maklumat rasmi di dalam BYOD;
- Menggunakan BYOD untuk mengakses, menyimpan dan menyebarkan maklumat rasmi dan terperingkat kepada pihak yang tidak dibenarkan;
- Menjadikan BYOD sebagai medium sandaran (backup) bagi maklumat rasmi;
- Merakam komunikasi dan dokumen rasmi untuk tujuan peribadi; dan
- Menjadikan BYOD sebagai access point kepada aset ICT jabatan untuk capaian ke Internet tanpa kebenaran.

vi. Pengguna adalah tertakluk kepada perkara seperti berikut:

- Menggunakan BYOD secara berhemah sepanjang masa dan mematuhi mana-mana peraturan/dasar yang berkuat kuasa;
- Memadamkan segala maklumat yang berkaitan dengan urusan rasmi jabatan sekiranya bertukar / ditamatkan perkhidmatan /

bersara ATAU sewaktu dihantar ke pusat servis untuk penyelenggaraan;

- Bertanggungjawab dan boleh dikenakan tindakan tatatertib sekiranya didapati menyalahgunakan BYOD yang menyebabkan kehilangan/ kerosakan/ pendedahan maklumat rasmi Kerajaan;
- UTMK berhak merampas mana-mana BYOD pengguna sekiranya didapati atau disyaki tidak mematuhi peraturan yang telah ditetapkan; dan
- UTMK tidak bertanggungjawab atas kehilangan, kerosakan data atau aplikasi dalam BYOD yang digunakan untuk tujuan urusan rasmi jabatan.

7 PENGURUSAN SISTEM APLIKASI

7.1 Sistem aplikasi yang digunapakai oleh pengguna HTJS terdiri daripada dua (2) kategori iaitu:

i. Sistem Penyumberan Luar (*Outsource*)
Sistem aplikasi atau perkhidmatan ICT yang dibangunkan, dihoskan, diselenggara atau diuruskan oleh pihak ketiga (kontraktor) bagi pihak HTJS atau KKM berdasarkan kontrak atau perjanjian perkhidmatan yang berkuat kuasa.

ii. Sistem Dalaman (*In-house*).
Sistem aplikasi atau perkhidmatan ICT yang dibangunkan, dihoskan, diselenggara dan diuruskan sepenuhnya oleh.

7.2 Pentadbir sistem aplikasi bertanggungjawab terhadap pengurusan pangkalan data, pengujian aplikasi, perubahan versi dan penyimpanan kod sumber.

7.3 Semua sistem aplikasi dan pangkalan data yang ditempatkan di HTJS atau yang dibangunkan secara dalaman adalah menjadi hakmilik HTJS.

7.4 Terdapat dua persekitaran dalam menyediakan sistem aplikasi iaitu Persekitaran Pembangunan serta Pengujian dan Persekitaran *Production*.

7.5 Semua tatacara ini adalah terpakai untuk sistem aplikasi dalaman yang dibangunkan oleh UTMK HTJS. Tatacara ini tidak meliputi sistem aplikasi yang dibangunkan oleh pihak ketiga dan sistem aplikasi yang dibekalkan oleh KKM.

7.6 TATACARA PERMOHONAN PEMBANGUNAN SISTEM APLIKASI BAHARU

i. Jabatan / unit yang memerlukan sistem aplikasi *in-house* baharu hendaklah mengemukakan permohonan rasmi melalui memo atau e-mel kepada UTMK beserta dokumen Borang Permohonan Pembangunan Sistem *In-house* (Lampiran D) yang telah lengkap diisi**.**

ii. Borang ini mesti ditandatangani oleh pemohon dan mendapat pengesahan serta cop daripada Ketua Jabatan / Unit sebelum diserahkan kepada UTMK untuk kelulusan.

7.7 TATACARA PENGUJIAN SISTEM APLIKASI

i. Bagi memastikan sistem aplikasi yang dibangunkan menepati spesifikasi dan kehendak pengguna, fasa pengujian hendaklah dilaksanakan sebelum sistem aplikasi *go-live*.

ii. UTMK akan menyediakan Borang Pengujian Penerimaan Pengguna (UAT) (Lampiran D). skrip pengujian dan diserahkan kepada pengguna semasa sesi Pengujian Penerimaan Pengguna (UAT). Pengguna akan melaksanakan pengujian dan merekodkannya di dalam borang tersebut. Segala penemuan ralat atau cadangan penambahbaikan semasa proses pengujian hendaklah direkodkan di dalam borang untuk tindakan pembetulan oleh UTMK.

iii. Setelah segala masalah dibaiki dan dipersetujui, Borang Pengujian Penerimaan Akhir (FAT) (Lampiran D) diisi bagi perakuan penerimaan sistem aplikasi berserta catatan atau ulasan, dan ia perlu ditandatangani oleh pegawai penerima beserta cop rasmi.

7.8 TATACARA PENYERAHAN SISTEM APLIKASI

i. UTMK akan menyerahkan sistem aplikasi yang telah siap dibangunkan kepada pemilik sistem aplikasi. Pengesahan penyerahan hendaklah dibuat menggunakan Borang Penyerahan Sistem Aplikasi (Lampiran D).

ii. Jabatan / unit penerima diwajibkan untuk menandatangani perakuan pada borang ini sebagai pengesahan penerimaan sistem aplikasi dan bersetuju untuk bertanggungjawab sepenuhnya terhadap penggunaan serta pengurusan sistem aplikasi tersebut.

iii. UTMK akan melaksanakan latihan kepada pengguna / pemilik aplikasi.

iv. Hebahan dan promosi pelaksanaan adalah di bawah tanggungjawab pemilik aplikasi.

7.9 TATACARA PENYELENGGARAAN DAN PENAMBAHBAIKAN SISTEM APLIKASI

Sekiranya terdapat masalah ralat, keperluan penyelenggaraan dan penambahbaikan ke atas modul sistem aplikasi sedia ada, pengguna hendaklah melengkapkan Borang Penyelenggaraan Sistem *Inhouse* (Lampiran D) dan diserahkan kepada UTMK**.**

7.10 TATACARA PENGURUSAN KESELAMATAN DATA: SANDARAN (*BACKUP*) & PEMULIHAN (*RESTORE*)

i. Bagi melindungi integriti data dan ketersediaan sistem aplikasi, UTMK hendaklah memastikan proses backup pangkalan data dan sistem aplikasi dilaksanakan dan direkodkan menggunakan Borang Log Backup Aplikasi Dan Pangkalan Data Sistem *Inhouse* (Lampiran D)**.**

ii. Proses restore pangkalan data dan sistem aplikasi hendaklah dilaksanakan sekurang-kurangnya sekali dalam tempoh satu (1) tahun atau mengikut keperluan dan direkodkan di dalam Borang Pemulihan (*Restore*) Aplikasi Dan Pangkalan Data (Lampiran D).

7.11 TATACARA PENAMATAN / PENANGGUHAN SISTEM APLIKASI

i. Penamatan atau penangguhan sistem aplikasi yang telah dibangunkan boleh dibuat oleh pemilik atau pembangun sistem aplikasi dengan menggunakan Borang Penamatan/Penangguhan Aplikasi (Lampiran D).

ii. Penamatan penggunaan sistem aplikasi hendaklah mengambil kira faktor seperti:
- tidak diguna pakai bagi tempoh enam (6) bulan;
- sistem aplikasi tidak menyokong proses kerja semasa;
- sistem aplikasi telah digantikan dengan sistem aplikasi baharu;
- sistem aplikasi tidak lagi disokong dari segi penyelenggaraan atau teknologi;
- terdapat risiko keselamatan ICT yang tidak dapat diterima; atau
- atas arahan KKM atau pihak pengurusan.

iii. UTMK hendaklah memaklumkan kepada pemilik sistem aplikasi mengenai penamatan / penangguhan sistem aplikasi dalam tempoh yang munasabah, termasuk tarikh akhir penggunaan.

iv. Semua rekod berkaitan penamatan / penangguhan sistem aplikasi hendaklah didokumenkan dan disimpan bagi tujuan rujukan, audit serta pematuhan.

v. Setelah sistem aplikasi ditamatkan pegawai yang bertanggungjawab perlu melaksanakan *backup* aplikasi dan pangkalan data ke dalam media storan dan diserahkan kepada Pentadbir Server UTMK untuk simpanan.

8 PENGURUSAN ID SISTEM APLIKASI DAN E-MEL RASMI

8.1 TATACARA PERMOHONAN ID SISTEM APLIKASI DAN E-MEL PENGGUNA BAHARU

Permohonan ID pengguna sistem aplikasi bagi kakitangan baharu yang berkhidmat di HTJS.

i. Pemohon hendaklah melengkapkan Borang Pendaftaran ID (Lampiran D), mendapatkan pengesahan Penyelia atau Ketua Jabatan / Unit dan menghantar borang permohonan kepada pihak UTMK.

ii. Pihak UTMK akan menerima dan menyemak borang tersebut. Pentadbir ID UTMK akan memproses dan mengemelkan slip ID kepada pembantu tadbir jabatan / unit atau e-mel alternatif pemohon dalam tempoh dua (2) hari bekerja dari tarikh permohonan diproses.

iii. Pengguna dikehendaki membuat percubaan log masuk ke dalam sistem aplikasi menggunakan ID tersebut dalam tempoh 24 jam, dan memaklumkan kepada UTMK sekiranya menghadapi sebarang masalah capaian.

8.2 Pengguna e-mel rasmi HTJS adalah tertakluk kepada **Pekeliling Pendigitalan Perkhidmatan Awam Bilangan 3 Tahun 2025 – Garis Panduan Tadbir Urus Perkhidmatan MyGovUC** dan **Surat Arahan Ketua Pengarah MAMPU 'Langkah-langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-agensi'** serta peraturan lain yang sedang berkuat kuasa.

8.3 Penghapusan ID e-mel boleh dilakukan:

i. Dalam tempoh **tujuh (7) hari** bekerja selepas tarikh pegawai keluar dari HTJS atas sebab bertukar kementerian, bersara, meletak jawatan atau menyambung pengajian.

ii. Penamatan ID bagi pengguna yang tidak aktif melebihi tempoh **sembilan puluh (90) hari**.

8.4 TATACARA PERMOHONAN AKSES DISIPLIN DAN *ROLE* SISTEM APLIKASI

i. Pemohon perlu melengkapkan Borang Permohonan Akses Disiplin dan Role Sistem (Lampiran D), mendapatkan pengesahan Ketua Jabatan / Unit dan menghantar borang permohonan kepada pihak UTMK.

ii. Pentadbir ID (UTMK) akan memproses borang yang diterima dan akan memaklumkan kepada pemohon.

8.5 PERMOHONAN AKSES KHAS

i. Bagi permohonan akses multidisiplin atau role tambahan oleh Pegawai Perubatan / Penolong Pegawai Perubatan / Pegawai Lantikan Kontrak / Jururawat, borang permohonan hendaklah disertakan dengan memo justifikasi daripada Ketua Jabatan / Unit.

ii. Bagi permohonan akses multidisiplin atau role tambahan oleh Pembantu Perawatan Kesihatan (PPK) atau Pembantu Tadbir (PT),

borang permohonan hendaklah disertakan dengan memo kelulusan daripada Pengarah.

iii. Bagi permohonan secara kelompok, permohonan boleh dikemukakan melalui memo daripada Ketua Jabatan / Unit atau Pengarah berserta senarai maklumat kakitangan yang memerlukan akses tersebut tanpa perlu mengemukakan borang permohonan individu, tertakluk kepada jawatan dan keperluan tugas.

8.6 PENAMATAN AKAUN PENGGUNA (*CLEARANCE*)

i. Pengguna yang akan menamatkan perkhidmatan di HTJS hendaklah melaksanakan proses *clearance* ID pengguna di UTMK. Pengguna hendaklah mengisi Borang Pendaftaran ID (Lampiran D) dengan menandakan pilihan "Hapus" pada bahagian Jenis Permohonan dengan catatan tarikh akhir perkhidmatan di HTJS.

ii. Penamatan akaun akan dilaksanakan dalam tempoh tiga (3) hari bekerja daripada tarikh akhir perkhidmatan di HTJS.

9 PENGURUSAN LATIHAN PEMANTAPAN PENGGUNAAN SISTEM APLIKASI

9.1 Tatacara ini bertujuan untuk menetapkan kaedah pengurusan latihan sistem aplikasi bagi memastikan semua pengguna mempunyai pengetahuan dan kemahiran yang mencukupi untuk menggunakan sistem aplikasi dengan berkesan dan selamat.

9.2 Tatacara ini terpakai kepada semua sistem aplikasi yang dibangunkan atau digunapakai di hospital serta melibatkan semua pengguna sistem aplikasi di jabatan / unit berkaitan.

9.3 Jabatan / unit hendaklah mengemukakan permohonan latihan kepada UTMK melalui memo rasmi atau emel dengan menyatakan maklumat berikut:

a. Nama sistem aplikasi
b. Bilangan & senarai Peserta
c. Tujuan latihan
d. Cadangan tarikh dan masa
e. Lokasi latihan

9.4 Pengurusan dan peruntukan (jika ada) berkaitan latihan adalah di bawah tanggung jawab pemohon / pemilik sistem aplikasi.

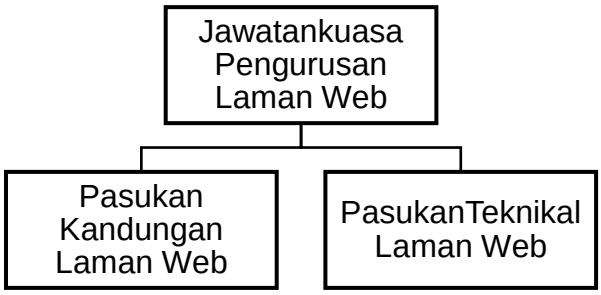
9.5 UTMK akan menyemak permohonan dan menyelaras jadual latihan berdasarkan keutamaan serta ketersediaan sumber.

9.6 Salinan rekod kehadiran latihan hendaklah diserahkan kepada UTMK sebagai rujukan.

10 PENGURUSAN LAMAN WEB HTJS

10.1 Tadbir urus laman web HTJS hendaklah dilaksanakan melalui Jawatankuasa Laman Web HTJS berdasarkan Pekeliling Pendigitalan Perkhidmatan Awam Bilangan 1 Tahun 2025 Pengurusan Portal/Laman Web Agensi Sektor Awam serta peraturan dan garis panduan yang berkuat kuasa.

10.2 Struktur tadbir urus Laman Web Rasmi HTJS adalah seperti yang ditunjukkan dalam rajah di bawah:



10.3 Jawatankuasa Laman Web HTJS hendaklah bertanggungjawab memastikan kandungan laman web sentiasa tepat, terkini, sahih, mudah diakses dan mematuhi keperluan keselamatan maklumat.

10.4 Pengguna yang ingin menerbitkan, mengemaskini atau meminda maklumat di laman web HTJS perlu mengemukakan permohonan menggunakan Borang Kemaskini Maklumat Laman Web Rasmi HTJS (Lampiran D). Permohonan hendaklah dikemukakan kepada UTMK melakui saluran rasmi yang ditetapkan.

10.5 Ketua jabatan / unit adalah bertanggungjawab sepenuhnya terhadap semua kandungan dan maklumat jabatan / unit masing-masing yang dipaparkan dalam laman web rasmi HTJS.

10.6 Laman web rasmi HTJS hanya digunakan bagi tujuan penyampain maklumat, perkhidmatan dan urusan rasmi HTJS sahaja.

10.7 Kandungan yang diterbitkan di laman web HTJS hendaklah mematuhi dasar, arahan, pekeliling dan peraturan KKM serta undang-undang yang berkuat kuasa. Kandungan yang mengandungi unsur keganasan, lucah, hasutan, fitnah, diskriminasi, kebencian, penghinaan, pelanggaran hak cipta atau apa-apa kandungan yang menyalahi undang-undang adalah dilarang.

11 PENGURUSAN KURSUS ICT

11.1 Perancangan kursus ICT hendaklah dilaksanakan berdasarkan keperluan organisasi, pembangunan kompetensi warga kerja, perubahan teknologi serta keutamaan perkhidmatan HTJS.

11.2 Semua penyertaan dalam kursus ICT hendaklah mendapat kelulusan Ketua Jabatan / Unit atau penyelia yang diberi kuasa mengikut peraturan yang berkuat kuasa.

11.3 Pengurusan peruntukan, pembayaran yuran, tuntutan dan perbelanjaan berkaitan kursus ICT hendaklah mematuhi peraturan kewangan, pekeliling dan garis panduan yang berkuat kuasa.

11.4 Rekod kehadiran dan penilaian keberkesanan kursus hendaklah diselenggara serta disimpan bagi tujuan pemantauan, audit dan rujukan.

11.5 Peserta kursus digalakkan berkongsi ilmu, kemahiran dan amalan terbaik yang diperoleh melalui sesi perkongsian ilmu, latihan dalaman, dokumentasi atau kaedah lain yang bersesuaian bagi meningkatkan kompetensi warga kerja HTJS.

11.6 Warga kerja HTJS hendaklah menghadiri latihan, taklimat atau program kesedaran ICT dan keselamatan siber yang diwajibkan oleh HTJS, KKM atau agensi berkaitan.

12 PENGURUSAN DOKUMENTASI ICT

12.1 Dokumentasi adalah termasuk tetapi tidak terhad kepada yang berikut:

i. Polisi ICT;
ii. *Standard Operating Procedures* (SOP);
iii. Manual pengguna;
iv. Pelan Kesinambungan Perkhidmatan (PKP);
v. Dokumen kualiti termasuk *Hospital Specific Approach* (HSA);
vi. Keperluan audit dan akreditasi;
vii. Laporan tahunan dan buletin;
viii. MyPortfolio;
ix. Pelan Tindakan dan Sasaran Kerja Utama;
x. Daftar aset dan rekod berkaitan Kew.PA; dan
xi. Surat menyurat dan memo

12.2 Semua dokumentasi ICT hendaklah disediakan mengikut format, piawaian dan templat yang ditetapkan serta dikemaskini secara berkala atau apabila berlaku perubahan sistem aplikasi, proses, dasar atau peraturan.

12.3 Setiap dokumentasi ICT hendaklah mempunyai kawalan versi, tarikh kuat kuasa, rekod pindaan dan kelulusan pihak yang diberi kuasa.

12.4 Dokumentasi ICT hendaklah disemak sekurang-kurangnya sekali dalam temph dua (2) tahun atau lebih awal sekiranya terdapat perubahan dasar, perundangan, teknologi, proses kerja atau keperluan organisasi.

13 PENGURUSAN KONTRAK PERKHIDMATAN ICT

13.1 Perolehan kontrak perkhidmatan ICT hendaklah dirancang berdasarkan keperluan organisasi, kesinambungan perkhidmatan, pengurusan risiko serta keutamaan operasi HTJS.

13.2 Semua urusan perolehan, pelantikan, pelaksanaan dan pengurusan pembekal perkhidmatan ICT hendaklah mematuhi peraturan kewangan, peraturan perolehan Kerajaan serta pekeliling yang berkuat kuasa.

13.3 Pembekal perkhidmatan ICT hendaklah mematuhi keperluan keselamatan maklumat HTJS, termasuk menandatangani Non-Disclosure Agreement (NDA) dan dokumen keselamatan lain yang berkaitan sebelum diberikan akses kepada aset ICT atau maklumat rasmi.

13.4 Prestasi pembekal hendaklah dipantau dan dinilai secara berkala berdasarkan SLA, petunjuk prestasi yang ditetapkan serta pematuhan terhadap syarat kontrak.

13.5 Sebarang perubahan terhadap skop kerja, kos, tempoh kontrak atau syarat kontrak hendaklah mendapat kelulusan pihak berkuasa yang berkaitan mengikut peraturan yang berkuat kuasa.

13.6 Pembaharuan, lanjutan atau penamatan kontrak hendaklah dirancang dan dilaksanakan secara teratur bagi memastikan kesinambungan perkhidmatan ICT serta mengelakkan gangguan kepada operasi HTJS.

13.7 Semua dokumen berkaitan kontrak ICT hendaklah direkodkan, disimpan, dilindungi dan dikawal mengikut Polisi Pengurusan Rekod HTJS serta peraturan yang berkuat kuasa.

13.8 Kontrak dan perkhidmatan ICT hendaklah tertakluk kepada pemantauan, semakan serta audit dalaman atau luaran bagi memastikan pematuhan terhadap Polisi ICT HTJS, syarat kontrak dan peraturan yang berkuat kuasa.

14 KHIDMAT MULTIMEDIA HTJS

14.1 TATACARA PERMOHONAN MULTIMEDIA HTJS

14.1.1 Permohonan multimedia adalah bagi aktiviti peringkat HTJS sahaja. Tugas multimedia hendaklah diselaras oleh UTMK dengan pemantauan pihak pengurusan HTJS.

14.1.2 Semua tugasan multimedia hendaklah dirancang dan dimohon secara rasmi melalui memo atau e-mel kepada Ketua UTMK selewat-lewatnya satu (1) bulan sebelum acara.

14.1.3 Kandungan multimedia hendaklah tepat, beretika, profesional dan tidak menjejaskan imej, keselamatan atau kerahsiaan hospital.

14.1.4 Rakaman melibatkan pesakit, waris atau kakitangan hendaklah mendapat kebenaran bertulis serta mematuhi perlindungan data dan privasi.

14.1.5 Penggunaan bahan multimedia hendaklah mematuhi undang-undang hak cipta dan harta intelek.

14.1.6 Persetujuan rekaan dan penyerahan bahan terakhir adalah seperti berikut:

i. Poster : **Dua (2) hari** sebelum acara
ii. Montaj : **Tujuh (7) hari** sebelum acara

14.1.7 Semua aktiviti multimedia hendaklah mematuhi dasar, polisi dan pekeliling yang berkuat kuasa.

15 HEBAHAN E-MEL DAN MEMO

15.1 PENGURUSAN HEBAHAN E-MEL DAN MEMO

15.1.1 Hebahan memo dan komunikasi rasmi HTJS hendaklah menggunakan e-mel rasmi MyGovcUC bagi memastikan penyampaian maklumat yang selamat, cekap dan berkesan.

15.1.2 Penggunaan e-mel rasmi sebagai medium penyampaian memo adalah bertujuan untuk:

i. mengurangkan penggunaan dokumen bercetak;
ii. meningkatkan kecekapan penyampaian maklumat dan urusan pentadbiran;
iii. menjimatkan kos, masa dan sumber; dan
iv. memastikan keselamatan serta kawalan edaran dokumen rasmi.

15.2 URUSETIA MEMO

15.2.1 Setiap jabatan / unit hendaklah melantik sekurang-kurangnya seorang Urusetia Memo bagi menguruskan penghantaran, penerimaan dan pengedaran memo rasmi melalui e-mel rasmi MOH.

15.2.2 Urusetia Memo bertanggungjawab untuk:

i. memantau e-mel rasmi yang diterima;
ii. mengambil tindakan yang sewajarnya terhadap memo yang diterima serta memanjangkannya kepada pegawai atau unit yang berkaitan; dan

iii. mengurus penghantaran memo rasmi kepada kumpulan e-mel yang berkenaan bagi memastikan edaran dibuat kepada penerima yang ditetapkan.

15.3 PENGURUSAN KUMPULAN E-MEL

15.3.1 Hebahan rasmi hendaklah menggunakan kumpulan e-mel rasmi yang diuruskan oleh HTJS.

15.3.2 Keahlian kumpulan e-mel hendaklah diselenggara dan dikemas kini secara berkala bagi memastikan ketepatan penerima hebahan.

15.3.3 Pengurusan kumpulan e-mel hendaklah dilaksanakan oleh pegawai yang diberi kuasa mengikut tatacara yang ditetapkan oleh HTJS.

15.4 PENGGUNAAN POSTMASTER HTJS

15.4.1 Akaun Postmaster HTJS hendaklah digunakan sebagai saluran rasmi untuk penyebaran maklumat, pengumuman dan notis kepada kakitangan HTJS yang mempunyai akaun e-mel rasmi MOH.

15.4.2 Penggunaan akaun Postmaster HTJS hendaklah terhad kepada penyebaran maklumat rasmi yang telah mendapat kelulusan pihak yang berkuasa.

15.5 PERMOHONAN HEBAHAN E-MEL

15.5.1 Sebarang permohonan hebahan melalui Postmaster HTJS hendaklah dikemukakan kepada UTMK mengikut tatacara dan saluran yang ditetapkan.

15.5.2 UTMK berhak menyemak kandungan hebahan bagi memastikan pematuhan terhadap dasar keselamatan ICT, peraturan yang berkuat kuasa dan kesesuaian penyebaran sebelum hebahan dilaksanakan.

C PENGUATKUASAAN DAN PEMATUHAN POLISI ICT

1 PEMAKAIAN

Polisi ICT HTJS 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 HTJS.

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

Sekiranya terdapat perbezaan Polisi ICT HTJS 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 HTJS.

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

2 PELANGGARAN POLISI

i. Setiap Pengguna di HTJS hendaklah membaca, memahami dan mematuhi Polisi ICT HTJS dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.
ii. Semua aset ICT di HTJS termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Pengarah HTJS berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.
iii. Sebarang pelanggaran Polisi yang melibatkan peralatan ICT atau maklumat data adalah merujuk kepada Prosidur Pengurusan Insiden HTJS

3 PENGECUALIAN

Sebarang pengecualian daripada mana-mana peruntukan dalam Polisi ICT ini hendaklah mendapat pertimbangan dan kelulusan Pengurusan Tertinggi HTJS dan UTMK HTJS.

4 TARIKH KUATKUASA

Polisi ICT HTJS adalah berkuat kuasa daripada tarikh ia diterbitkan.

LAMPIRAN A

SURAT AKUAN PEMATUHAN POLISI ICT HTJS

SURAT AKUAN PEMATUHAN POLISI ICT

HOSPITAL TUANKU JA'AFAR (HTJ)

Nama Penuh
(Huruf Besar) :.....

No. Kad Pengenalan :.....

Jawatan/Gred :.....

Jabatan/Unit :.....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi ICT HTJ, 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 (ICTSO)

.....
(Nama Pegawai Keselamatan ICT)
b.p.Pengarah Hospital Tuanku Ja'afar

Tarikh :.....

LAMPIRAN B

SURAT LANTIKAN CDO

KEMENTERIAN KESIHATAN MALAYSIA

HOSPITAL TUANKU JA'AFAR
(TUANKU JA'AFAR HOSPITAL)
Jalan Rasah
70300 Seremban
NEGERI SEMBILAN
MALAYSIA

Kami Sedia Membantu
KEMENTERIAN KESIHATAN MALAYSIA

Tel : 06-768 4000 (40 talian / *lines*)
Faks : 06-762 5771
Laman Web : www.htjs.moh.gov.my

Ruj. Kami : HTJS 106/193 JLD 10 (33)
Tarikh : 16 Januari 2026

Dr. Zuhaida binti Che Embi
Timbalan Pengarah Perubatan I
Hospital Tuanku Ja'afar
Seremban, Negeri Sembilan

YBrs Dr,

PELANTIKAN SEBAGAI *CHIEF DIGITAL OFFICER* (CDO), HOSPITAL TUANKU JA'AFAR, SEREMBAN (HTJS)

Dengan hormatnya saya merujuk kepada perkara di atas.

2. Sukacita dimaklumkan bahawa pihak pengurusan HTJS dengan ini melantik YBrs Dr. sebagai ***Chief Digital Officer*** **(CDO)** HTJS berkuat kuasa serta-merta.

3. Pelantikan ini adalah selaras dengan keperluan tadbir urus pendigitalan sektor awam dan bertujuan untuk memperkukuhkan perancangan serta pelaksanaan transformasi digital hospital selaras dengan dasar dan garis panduan Kerajaan.

4. Tanggungjawab CDO adalah termasuk tetapi tidak terhad kepada:

- Menetapkan hala tuju dan strategi pendigitalan hospital
- Menyelaras inisiatif transformasi digital dan inovasi ICT
- Memastikan pelaksanaan ICT selaras dengan keperluan operasi, keselamatan maklumat dan pematuhan dasar Kerajaan
- Memberi nasihat strategik kepada pihak pengurusan berkaitan teknologi digital

5. Pihak pengurusan berharap YBrs Dr. dapat melaksanakan amanah ini dengan penuh komitmen profesionalisme dan integriti demi meningkatkan kecekapan perkhidmatan digital hospital.

Sekian, terima kasih.

"MALAYSIA MADANI"

"BERKHIDMAT UNTUK NEGARA"

Saya yang menjalankan amanah,

(DATO' DR. ZALEHA BINTI MD NOOR)
Pengarah
Hospital Tuanku Ja'afar, Seremban

LAMPIRAN C

SURAT LANTIKAN ICTSO

KEMENTERIAN KESIHATAN MALAYSIA

HOSPITAL TUANKU JA'AFAR
(TUANKU JA'AFAR HOSPITAL)
Jalan Rasah
70300 Seremban
NEGERI SEMBILAN
MALAYSIA

Kami Sedia Membantu
KEMENTERIAN KESIHATAN MALAYSIA

Tel : 06-768 4000 (40 talian / *lines*)
Faks : 06-762 5771
Laman Web : www.htjs.moh.gov.my

Ruj. Kami : HTJS 106/193 JLD 10 (32)
Tarikh : 16 Januari 2026

Puan Raihayu binti Abd Rahman
Ketua Penolong Pengarah (ICT)
Hospital Tuanku Ja'afar
Seremban, Negeri Sembilan

Puan,

PELANTIKAN SEBAGAI *ICT SECURITY OFFICER* (ICTSO), HOSPITAL TUANKU JA'AFAR, SEREMBAN (HTJS)

Dengan hormatnya saya merujuk kepada perkara di atas.

2. Sukacita dimaklumkan bahawa pihak pengurusan HTJS dengan ini melantik Puan sebagai ***ICT Security Officer (ICTSO)*** HTJS berkuat kuasa serta-merta.

3. Pelantikan ini dibuat bagi memastikan pengurusan dan kawalan keselamatan maklumat serta keselamatan ICT hospital dilaksanakan secara berkesan dan berterusan selaras dengan dasar dan garis panduan Kerajaan.

4. Tanggungjawab ICTSO adalah termasuk tetapi tidak terhad kepada:

- Menyelaras pelaksanaan dasar dan kawalan keselamatan ICT hospital
- Mengenal pasti, menilai dan memantau risiko keselamatan maklumat
- Menyelaras pengurusan insiden keselamatan ICT
- Memantau pematuhan audit keselamatan ICT dan ISMS
- Bertindak sebagai pegawai rujukan keselamatan ICT hospital

5. Pihak pengurusan berharap Puan dapat melaksanakan amanah ini dengan penuh komitmen profesionalisme dan integriti bagi memastikan kerahsiaan, integriti dan ketersediaan maklumat hospital sentiasa terpelihara.

Sekian, terima kasih.

"MALAYSIA MADANI"

"BERKHIDMAT UNTUK NEGARA"

Saya yang menjalankan amanah,

(DATO' DR. ZALEHA BINTI MD NOOR)
Pengarah
Hospital Tuanku Ja'afar, Seremban

LAMPIRAN D

SENARAI BORANG

Kementerian Kesihatan Malaysia

BORANG PENDAFTARAN ID

Unit Teknologi Maklumat & Komunikasi
Hospital Tuanku Ja'afar, Seremban

Sila lengkapkan Bahagian 1 dan 2 (Semua Bahagian adalah WAJIB)

BAHAGIAN 1: MAKLUMAT PEMOHON

Jenis Permohonan : ☐ Baru ☐ Set semula kata laluan ☐ Hapus: (sila nyatakan sebab) .....

☐ Dr. Nama : _____ No. Kad Pengenalan : _____
Tanda √ jika berkaitan

Jawatan : _____ Gred : _____ No. MMC/REG: _____

No Telefon : _____ (HP) _____ (P) Tarikh Lahir : _____

Jantina : ○ Lelaki ○ Perempuan Status Perkahwinan : ○ Bujang ○ Berkahwin

E-mel MOH : _____ @moh.gov.my E-mel Alternatif : _____

Sistem : HIS@KKM ☐ CenSSIS ☐ OTMS ☐ LIS ☐ SPP ☐ E-mel ☐ Lain-lain (Nyatakan) : _____

Jabatan / Bahagian / Unit :

- ○ Jabatan Perubatan Dalaman
- ○ Jabatan Nefrologi
- ○ Jabatan Perubatan Transfusi
- ○ Jabatan Dermatologi
- ○ Jabatan Perubatan Rehabilitasi
- ○ Jabatan Psikiatri
- ○ Jabatan Perubatan & Kesihatan Pekerjaan
- ○ Jabatan Kecemasan & Trauma
- ○ Jabatan Anestesiologi & Rawatan Kritikal
- ○ Jabatan Pembedahan Am
- ○ Jabatan Pembedahan Saraf
- ○ Jabatan Ortopedik
- ○ Jabatan Oftalmologi
- ○ Jabatan Otorinolaringologi
- ○ Jabatan Obstetrik & Ginekologi
- ○ Jabatan Pediatrik
- ○ Jabatan Pergigian Pediatrik
- ○ Jabatan Bedah Mulut & Maksilofasial
- ○ Jabatan Radiologi
- ○ Jabatan Patologi
- ○ Jabatan Forensik
- ○ Jabatan Farmasi
- ○ Jabatan Rekod Perubatan
- ○ Jabatan Dietetik & Sajian
- ○ Jabatan Kerja Sosial
- ○ Unit Kejuruteraan
- ○ Unit Pengurusan Risiko dan Survelan Klinikal
- ○ Unit Dasar Perubatan & Perancangan Perkhidmatan Klinikal
- ○ Unit Perkembangan Profesion Pakar & Pegawai Perubatan
- ○ Unit Kesihatan Awam
- ○ Unit Kejururawatan
- ○ Unit Penyeliaan Hospital
- ○ Unit Penyelidikan Klinikal
- ○ Unit Bekalan Bahan Steril
- ○ Unit Kawalan Infeksi
- ○ Unit Kewangan
- ○ Unit Hasil
- ○ Unit Pembangunan
- ○ Unit Keselamatan
- ○ Unit Pentadbiran
- ○ Unit Sumber Manusia
- ○ Unit Perpustakaan Perubatan
- ○ Unit Perhubungan Awam & Khidmat Pelanggan
- ○ Unit Perolehan
- ○ Unit Pengurusan Aset & Stor
- ○ Unit Latihan & Perkembangan Kerjaya
- ○ Unit Hal Ehwal Islam
- ○ Unit Teknologi Maklumat & Komunikasi

Lokasi : _____

BAHAGIAN 2: PENGESAHAN

Saya dengan ini memahami dan bersetuju dengan terma yang ditetapkan dalam sistem-sistem tersebut dan saya tidak akan berkongsi ID pengguna. Jika saya didapati menyalahgunakan ID pengguna, tindakan tatatertib akan diambil ke atas saya.

Tandatangan Pemohon	**Tandatangan Penyelia / Ketua Jabatan/Unit**
Tarikh :	Tarikh :

BAHAGIAN 3 : UNTUK KEGUNAAN UNIT TEKNOLOGI MAKLUMAT & KOMUNIKASI

Tarikh & Masa Terima : _____

Tarikh & Masa Selesai : _____

Cop Pendaftar :

ISSUE LOG HIS

Complaint Number		**Period of complaint**	☐ During Office Hour ☐ After Office Hour		
Ward / Clinic			**Ext. No.**		
Request By		**Request Date**		**Request Time**	
Patient Name			**MRN No**		
Issue / Problem	**Date of Admit**		**Date of Discharge**		
	☐ Correction of Discharge Summary		☐ CIS Order		
	☐ Medical Record		☐ Correction on Date of Discharge		
	☐ Billing / Unit Hasil		☐ Others		
	System : ☐ SPP ☐ OTMS ☐ CENSSIS ☐ LIS ☐ RIS ☐ OBSCENTRAL ☐ OTHERS (PLEASE SPECIFY) _____				
	Description :				
	Request by User : **Name :** **Designation :** **Signature :** **Date :**		**Acknowledgement By Supervisor :** **Name :** **Designation :** **Signature :** **Date :**		
FOR OFFICE USE :	**Received By**		**Date Received**		**Time**
	Escalated To		**Escalated Date**		**Time**
	Log Category	☐ System Bug ☐ User Faulty			
	Ticket No		**Job Sheet No**		
	Remarks :			**Date Solved**	
				Time Solved	
				Signature	
				No Ticket	

HTJS/ICT/BRG 003

BORANG PENGESAHAN ICT

UNIT TEKNOLOGI MAKLUMAT DAN KOMUNIKASI
HOSPITAL TUANKU JA'AFAR SEREMBAN

☐ **PEMULANGAN PERKAKASAN**

☐ **PENYERAHAN PERKAKASAN**

☐ **PEMASANGAN PERISIAN**

☐ **LAIN LAIN**

A. MAKLUMAT PENGGUNA

i. Nama Penerima : _____

ii. Jawatan: _____

iii. Jabatan / Unit / Klinik / Wad: _____

v. No.Telefon : (H/P) _____ Samb: _____

B. MAKLUMAT PERALATAN ICT

i. Model/Jenama:

ii. Processor :

iii. RAM:

iv. HDD:

v. Monitor:

vi. Tag ID Perkakasan:

vii. CPU- Serial Number:

viii. Monitor-Serial Number:

ix. Printer-Serial Number:

x. Computer Hostname:

C. Lain-lain

_____

_____

_____

HTJS/ICT/BRG 003

SENARAI SEMAK PERALATAN

1. PERKAKASAN

CPU	ABLE TO ON	☐ YES	☐ NO
MONITOR	ABLE TO ON	☐ YES	☐ NO
KEYBOARD / MOUSE	ABLE TO ON	☐ YES	☐ NO
SPEAKER	ABLE TO ON	☐ YES	☐ NO
PRINTER	ABLE TO ON	☐ YES	☐ NO
HARDDISK PARTITION		☐ DRIVE C	☐ DRIVE D

2. PERISIAN

i. OPERATING SYSTEM	☐ WIN XP	☐ WIN VISTA	☐ WIN 7	☐ WIN 8/8.1	☐ WIN 10
ii. OFFICE AUTOMATION	☐ MICROSOFT OFFICE		☐ OPEN OFFICE	☐ KINGSOFT OFFICE	
iii. ANTIVIRUS	☐ TREND MICRO		☐ AVIRA	☐ KASPERSKY	
	☐ F-SECURE		☐ SMADAV	☐ LAIN LAIN	
iv. PDF READER	☐ ADOBE		☐ NITRO PDF	☐ PDF EXPRESS	
v. INTERNET BROWSER	☐ INTERNET EXPLORER		☐ GOOGLE CHROME	☐ FIREFOX	
vi. ZIP COMPRESSION	☐ WINRAR		☐ WINZIP		
vii. INSTALL JAVA			☐ YES	☐ NO	
viii. 1GOVUC	ENTERPRISE TRUST		☐ YES	☐ NO	
	ROOT CA		☐ YES	☐ NO	

3. LAIN-LAIN

i. ABLE TO CONNECT TO INTERNET		☐ YES	☐ NO
ii. INSTALL PRINTER	MODEL: _____	☐ YES	☐ NO
iii. TESTED PRINT		☐ YES	☐ NO

4 CATITAN

_____

_____

_____

PENGESAHAN PEGAWAI BERTANGGUNGJAWAB

Tandatangan: _____

NAMA PEGAWAI: _____

TARIKH: _____

PENGESAHAN PENGGUNA:

Tandatangan: _____

NAMA PENERIMA: _____

TARIKH: _____

SAYA MENGESAHKAN BAHAWA KERJA-KERJA YANG DIPERTANGGUNGJAWABKAN ADALAH LENGKAP DAN SEMPURNA

Tandatangan: _____

NAMA: _____

(pegawai gred F41 dan ke atas)

JAWATAN: _____

TARIKH: _____

Unit Teknologi Maklumat & Komunikasi

BORANG PENGESAHAN LATIHAN ICT BAGI KAKITANGAN HTJS

TARIKH : _____

MASA : _____

PERKARA : _____

_____

1. _____ (T/T *PENERIMA LATIHAN*)

   NAMA : _____

   JAWATAN (GRED) : _____

   NO K/P : _____

   UNIT / JABATAN : _____

2. _____ (T/T *PENYELIA*)

   NAMA : _____

   JAWATAN (GRED) : _____

3. _____ (T/T *PEGAWAI IT*)

   NAMA : _____

   JAWATAN (GRED) : _____

UNIT TEKNOLOGI MAKLUMAT & KOMUNIKASI
HOSPITAL TUANKU JA'AFAR, SEREMBAN

BORANG PENILAIAN PRESTASI PEMBEKAL

A. MAKLUMAT PEMBEKAL

1. **Nama & Alamat Pembekal :**
2. **Tajuk Kerja/ Bekalan/Perkhidmatan :**
3. **Jumlah Harga Tawaran :**

B. PRESTASI PEMBEKAL

Penilaian dikehendaki memberikan Penilaian Prestasi Pembekal berasaskan penjelasan kriteria (1-5) yang dinyatakan dibawah. Setiap kriteria diberi markah penug sebanyak 20 markah :-

BIL	KRITERIA	MARKAH	CATATAN
1	**HARGA** Kesesuaian mengikut harga semasa		
2	**KUALITI** Memenuhi ekspektasi Pelanggan		
3	**MASA** Dihantar/dilaksanakan dalam tempoh yang ditetapkan		
4	**PERKHIDMATAN** Kesempurnaan kerja-kerja yang dilaksanakan		
5	**KEMAHIRAN** Pengetahuan dalam bidang kerja.		
	JUMLAH MARKAH (Markah Penuh 100)		

PENGUKURAN PENILAIAN PRESTASI PEMBEKAL (tandakan (x))		KRITERIA YANG DITERIMA / PERTIMBANGKAN
80 hingga 100 - Baik	☐	Diterima dan dikekalkan dalam senarai pembekal
60 hingga 79 - Memuaskan		
40 hingga 59 - Sederhana	☐	Di dalam perhatian
Dibawah 40 - Tidak Memuaskan	☐	Disyorkan untuk disenarai hitam

ULASAN KESELURUHAN & PENGESAHAN PENILAI

.....

.....

Tandatangan :
Nama :
Jawatan :
Tarikh :

KEGUNAAN SUB/TSUB /KETUA CAWANGAN/KETUA UNIT

SOKONG / TIDAK SOKONG

Tandatangan :

Nama :
Jawatan :
Tarikh :

UNIT TEKNOLOGI MAKLUMAT & KOMUNIKASI
HOSPITAL TUANKU JA'AFAR SEREMBAN, NEGERI SEMBILAN

BORANG PERMOHONAN PEMBANGUNAN SISTEM *INHOUSE*

****Sila isi maklumat menggunakan **HURUF BESAR***

Maklumat Permohonan

Nama :			
Jawatan :		Emel :	
Unit / Jabatan :		Tarikh :	
Tujuan / Objektif :	(Sila buat lampiran jika ruang tidak mencukupi)		

Sila kepilkan lampiran bagi perkara-perkara berikut: Tandakan (/)

1. Kertas Kerja
   - Skop / Spesifikasi / Objektif / Fungsi / Pernyataan Masalah / Sasaran Pengguna ☐
   - Rajah / carta alir proses kerja ☐
   - Penerangan keseluruhan rajah / carta alir proses kerja ☐
   - Contoh dokumen input yang sedia ada (borang-borang berkaitan) ☐
   - Contoh format laporan yang perlu dijana ☐

PENGAKUAN PEMOHON

Saya dengan ini memohon UTMK menyediakan satu sistem baru seperti yang dinyatakan di atas. Segala prosedur yang ditetapkan telah saya baca dan fahami, dan bersetuju untuk mematuhinya.

…… ……

Tandatangan Pemohon Tandatangan & Cop Ketua Unit / Jabatan

Tarikh : Tarikh :

Untuk Kegunaan Unit Teknologi Maklumat & Komunikasi (UTMK) Sahaja

Status Permohonan **Tarikh Terima Permohonan : ……..**

☐ Diluluskan ☐ Dalam Pertimbangan ☐ Dokumen Tidak Lengkap ☐ Tidak Diluluskan

Catatan :

Tarikh makluman melalui emel : (Sila buat lampiran jika ruang tidak mencukupi)

Tarikh Diterima :	**Tarikh Disemak :**	**Tarikh Disah:**
……	……	……
Tandatangan & Cop PPTM	Tandatangan & Cop PPK (SSAL)	Tandatangan & Cop KPP (ICT)
Nama :	Nama :	Nama :

Borang yang telah lengkap diisi hendaklah diserahkan ke Unit Teknologi Maklumat & Komunikasi. Segala dokumen berkaitan (minit mesyuarat / emel / catatan dan sebagainya) perlu dikepilkan bersama borang permohonan.

Kementerian Kesihatan Malaysia

UNIT TEKNOLOGI MAKLUMAT & KOMUNIKASI
HOSPITAL TUANKU JA'AFAR, SEREMBAN

BORANG PENYELENGGARAAN SISTEM *INHOUSE*
NAMA SISTEM : ……

****Sila isi maklumat menggunakan **HURUF BESAR***

Maklumat Permohonan

Nama :			
Jawatan :		E-mel :	
Unit / Jabatan :		Tarikh :	
Kategori :	☐ Penyelenggaraan ☐ Penambahbaikan Sila nyatakan modul sistem yang ingin ditambah / digugurkan		
A. Catatan Penyelenggaraan / Permasalahan :	(Sila buat lampiran jika ruang tidak mencukupi)		

B. Sila kepilkan lampiran bagi perkara-perkara berikut: Tandakan (/)

1. Rajah / carta alir proses kerja ☐
2. Penerangan keseluruhan rajah / carta alir proses kerja ☐
3. Contoh dokumen input yang sedia ada (borang-borang berkaitan) ☐
4. Contoh format laporan yang perlu dijana ☐

PENGAKUAN PEMOHON

Saya dengan ini memahami segala prosedur yang telah ditetapkan dan bersetuju untuk mematuhinya

…… ……

Tandatangan Pemohon Tandatangan & Cop Ketua Unit / Jabatan

Tarikh : Tarikh :

Untuk Kegunaan Unit Teknologi Maklumat & Komunikasi Sahaja

Status Permohonan **Tarikh Terima Permohonan : ……..**

Tindakan / Ulasan : Tarikh Selesai :

(Sila buat lampiran jika ruang tidak mencukupi)

Tindakan Oleh :	**Disemak Oleh :**	**Disahkan Oleh :**	**Diluluskan Oleh :**
……	……	……	……
Tandatangan & Cop PPTM	Tandatangan & Cop Pemohon	Tandatangan & Cop PTM	Tandatangan & Cop KUTMK
Nama :	Nama :	Nama :	Nama :
Tarikh :	Tarikh :	Tarikh :	Tarikh :

Borang yang telah lengkap diisi hendaklah diserahkan ke Unit Teknologi Maklumat & Komunikasi. Segala dokumen berkaitan (minit mesyuarat / e-mel / catatan dan sebagainya) perlu dikepilkan bersama borang permohonan.

BORANG LOG PENGURUSAN SERVER

HTJS/ICT/BRG 008

1. MAKLUMAT SERVER					
a. Nama Server	:				
b. CPU	:				
c. RAM	:	GB	d. Alamat I.P	:	
e. Hard Disk	:	C:/ GB	D:/ GB		
f. Nama Pengguna	:	1)			
		2)			
		3)			
		4)			

2. PEMANTAUAN PENGURUSAN SERVER					
Bil	Item	Mac	Jun	Sept	Dis
a.	*CPU Utilization* (%)				
b.	*RAM Utilization* (%)				
c.	*Hard Disk Utilization* (%)				
	Tandatangan				

3. PENYELENGGARAAN CAKERA KERAS					
Bil	Item	Mac	Jun	Sept	Dis
a.	*Error Checking*				
b.	*Defragmantation*				
	Tandatangan				

4. PENGURUSAN KESELAMATAN SERVER					
Bil	Item	Mac	Jun	Sept	Dis
a.	Antivirus (*Scan/Update*)				
b.	Penukaran Katalaluan				
	Tandatangan				

5. PENGEMASKINIAN WINDOWS					
Bil	Item	Mac	Jun	Sept	Dis
a.	Pengemaskinian Windows				
	Tandatangan				

6. KERJA-KERJA PEMBERSIHAN FIZIKAL

Nama Pegawai : _____ Tarikh : _____

Tandatangan : _____

BORANG LOG PENGURUSAN SERVER

HTJS/ICT/BRG 008

7. PEMANTAUAN EVENT LOG				
Bulan	Log	Bil Critical	Catatan	Tandatangan
Januari	*Application*			
	Security			
	System			Tarikh :
Februari	*Application*			
	Security			
	System			Tarikh :
Mac	*Application*			
	Security			
	System			Tarikh :
April	*Application*			
	Security			
	System			Tarikh :
Jun	*Application*			
	Security			
	System			Tarikh :
Julai	*Application*			
	Security			
	System			Tarikh :
Ogos	*Application*			
	Security			
	System			Tarikh :
September	*Application*			
	Security			
	System			Tarikh :
Oktober	*Application*			
	Security			
	System			Tarikh :
November	*Application*			
	Security			
	System			Tarikh :
Disember	*Application*			
	Security			
	System			Tarikh :

BORANG LOG *BACKUP* APLIKASI DAN PANGKALAN DATA SISTEM *INHOUSE*
Unit Teknologi Maklumat & Komunikasi (UTMK)
Hospital Tuanku Ja'afar, Seremban

NAMA SISTEM: _____

TARIKH *BACKUP*	MASA *BACKUP*	KATEGORI BACKUP	CATATAN	NAMA & TANDATANGAN
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		

TARIKH *BACKUP*	MASA *BACKUP*	KATEGORI BACKUP	CATATAN	NAMA & TANDATANGAN
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		
		☐ Aplikasi ☐ Pangkalan Data		

BORANG PEMULIHAN (*RESTORE)* APLIKASI DAN PANGKALAN DATA SISTEM *INHOUSE*

Unit Teknologi Maklumat & Komunikasi (UTMK)

Hospital Tuanku Ja'afar, Seremban

Nama Server	
Nama Sistem Aplikasi	
Tarikh Folder/ Fail Aplikasi	
Nama Pangkalan Data	
Tarikh Pangkalan Data	
Tujuan Pemulihan Dilaksanakan	
Persekitaran Pemulihan	
Tarikh dan Masa Pemulihan Dilaksanakan	
Status Pemulihan	☐ Berjaya ☐ Berjaya Sebahagian ☐ Tidak berjaya
Catatan/ Ulasan	

PEGAWAI YANG BERTANGGUNGJAWAB

Tandatangan:

Nama:

Jawatan:

Tarikh:

PENGESAHAN PENYELIA/ KETUA UNIT

Tandatangan:

Nama:

Jawatan:

Tarikh:

BORANG PENGURUSAN KAWALAN PERUBAHAN

HTJS/ICT/BRG 011

A. MAKLUMAT PEMOHON DAN SERVER		
Nama Pemohon		
Jawatan / Seksyen		
Tarikh		
Maklumat Server	Nama Server	
	IP	
	Sistem terlibat	
	Domain	

B. MAKLUMAT PERUBAHAN

☐ PERKAKASAN ☐ PERISIAN

No.	Butiran Semasa	Cadangan Perubahan

Tandatangan Pemohon :

C. KEPUTUSAN KAJIAN AWAL PERMINTAAN PERUBAHAN

☐ LULUS ☐ TOLAK ☐ TANGGUH

Catatan :

Tandatangan	
Nama Penyemak	
Tarikh	

D. KELULUSAN PERMOHONAN

☐ LULUS ☐ TOLAK

Catatan :

Diluluskan oleh	
Tandatangan	:
Nama	:
Tarikh	:

Kementerian Kesihatan Malaysia

BORANG KEMASKINI MAKLUMAT LAMAN WEB HTJS

Unit Teknologi Maklumat & Komunikasi
Hospital Tuanku Ja'afar, Seremban

MAKLUMAT PEMOHON

Nama : _____

Jabatan / Unit : _____

E-mel : _____

Ext. _____

MAKLUMAT PENGEMASKINIAN LAMAN WEB

Tandakan √ pada yang berkenaan:

Maklumat Baru	
Maklumat Tambahan / Pengemaskinian Maklumat	
Cadangan / Pindaan	

Kategori:

	Banner		Laporan Tahunan		Direktori
	Pengumuman / Berita		Borang		Lain-Lain (Sila nyatakan)
	Sebut Harga / Tender		Sumber Rujukan		
	Maklumat Korporat		Gambar		
	Maklumat Jabatan / Unit		Video		

Perkara : _____

_____

Tarikh Paparan : _____

Sila lampirkan bersama perincian pengemaskinian dan hantar ke UTMK atau e-melkan kepada:* ***webmasterhtjs@moh.gov.my*

Disediakan oleh	**Disahkan oleh**
(Nama, Cop & Tandatangan)	**(Nama, Cop & Tandatangan)**

UNTUK KEGUNAAN UNIT TEKNOLOGI MAKLUMAT & KOMUNIKASI

Status permohonan : **LULUS / DITOLAK**

Tarikh terima : _____

Tarikh kemaskini : _____

Dikemaskini oleh : _____

Catatan : _____

Kementerian Kesihatan Malaysia

BORANG PERMOHONAN AKSES DISIPLIN DAN ROLE SISTEM

Unit Teknologi Maklumat & Komunikasi
Hospital Tuanku Ja'afar, Seremban

Sila lengkapkan maklumat di bawah :

BAHAGIAN 1: MAKLUMAT PEMOHON

☐ Dr. Nama : _____ No. Kad Pengenalan : _____
Tanda √ jika berkaitan

Jawatan : _____ Gred : _____ No. MMC/REG: _____

No Telefon : _____ (HP) _____ (P) E-mel MOH : _____ @moh.gov.my

Sistem Semasa yang Digunakan : ☐ SPP

HIS@KKM
☐ CenSSIS ☐ OTMS ☐ LIS

Disiplin Semasa (Optional): _____ Role Semasa (Optional) : _____

Capaian Disiplin Tambahan (SPP)		**Capaian Role Tambahan**	
☐ Anaesthesiology	☐ Oral Maxillofacial Surgery	**SPP**	**OTMS**
☐ Dermatology	☐ Orthopaedic	☐ Medical Officer	☐ Anaest
☐ Emergency Medicine	☐ Otorhinolaryngology	☐ Jururawat	☐ ORNurse
☐ Endocrinology	☐ Paediatric	☐ Pen. Pegawai Perubatan	☐ Surgeon
☐ Forensic Medicine	☐ Paediatric Surgery	☐ Pem. Perawatan Kesihatan	☐ Ward
☐ Gastroenterology	☐ Paediatric Dentistry	☐ Authorized Radiology Order	
☐ General Medicine	☐ Psychiatry		**CenSSIS**
☐ General Surgery	☐ Radiology	☐ Lain-lain (**Nyatakan**)	☐ Admin
☐ Geriatric	☐ Rehabilitative Medicine		☐ Receive
☐ Gynaecology	☐ Respiratory Medicine	_____	☐ User
☐ Haematology	☐ Rheumatology		☐ Staff
☐ Infectious Disease	☐ Sport Medicine	**LIS**	☐ Supervisor
☐ Nephrology	☐ Multidiscipline*	☐ Lab User	☐ SV Assistant
☐ Neurology	***Memo Justifikasi HOD**	☐ Ward Clinician	
☐ Neurosurgery			
☐ Obstetric			
☐ Ophthalmology			

BAHAGIAN 2: PENGESAHAN

Saya dengan ini memahami dan bersetuju dengan terma yang ditetapkan dalam sistem-sistem tersebut dan saya tidak akan berkongsi ID pengguna. Jika saya didapati menyalahgunakan ID pengguna, tindakan tatatertib akan diambil ke atas saya.

Tandatangan Pemohon	**Tandatangan Ketua Jabatan**
Tarikh :	Tarikh :

BAHAGIAN 3 : UNTUK KEGUNAAN UNIT TEKNOLOGI MAKLUMAT & KOMUNIKASI

Tarikh & Masa Terima : _____

Tarikh & Masa Selesai : _____

Cop Pendaftar :

UNIT TEKNOLOGI MAKLUMAT DAN KOMUNIKASI
HOSPITAL TUANKU JA'AFAR SEREMBAN

BORANG TEMPAHAN MAKMAL ICT BLOK CEMPAKA

* Borang hendaklah diisi dengan lengkap dan mematuhi syarat-syarat tempahan ditetapkan

Untuk Kegunaan Pejabat	
No. Rujukan	

1.	**BUTIR DIRI PEMOHON**

Nama : ……

Jabatan : …… No. Telefon/HP: ……

2.	**BUTIR TEMPAHAN**

Tujuan : ……

……..
(sila nyatakan nama mesyuarat/kursus/taklimat/lain-lain dengan lengkap)

Tarikh : ……hingga ……..

Masa : …… hingga ……..

Bil. Peserta.....orang

3.	**KEPERLUAN KEMUDAHAN ICT**

NO.	PERALATAN ICT	TANDAKAN (✓)
1.	Komputer / Laptop	
2.	Mikrofon dan Pembesar Suara	

…….. Tarikh: ……..
(Tandatangan Pemohon)

4.	**PEMBATALAN (Dimaklumkan seminggu sebelum tarikh tempahan)**

Sebab Pembatalan : ……

…….. ……

(Tandatangan Pembatal) (Pengesahan Unit Teknologi Maklumat)

Tarikh : ……

PKP BORANG PENDAFTARAN PESAKIT
(UMUM)

LOKASI : _____

NO. DAFTAR SEMENTARA (RN)	TARIKH DAFTAR	MASA DAFTAR	ZON (ED Sahaja)	NAMA PESAKIT	NO. KAD PENGENALAN / PASSPORT	TARIKH LAHIR	UMUR	JANTINA	WARGA NEGARA	BANGSA	*MARRIED TO LOCAL* (Jika bukan warganegara)	ALAMAT	NO. TEL	NO. RESIT

PKP BORANG PENDAFTARAN PESAKIT
UNIT DAFTAR MASUK (UDM)

NO. DAFTAR SEMENTARA (RN)	TARIKH DAFTAR	MASA DAFTAR	NAMA PESAKIT	NO. KAD PENGENALAN/ PASSPORT	WARGA NEGARA	BUKAN WARGA NEGARA	*MARRIED TO LOCAL* (Jika bukan warganegara)	ALAMAT	NO. TEL	JUMLAH DEPOSIT	NO. RESIT	LOKASI (WAD)

PKP DISPATCHED LIST LABORATORY ORDER

LOKASI : _____

NO	IDENTIFICATION	MRN	PATIENT NAME	TEST NAME	DIAGNOSIS	PRIORITY	QUANTITY	REQUESTED BY	REQUESTED DATE

PKP BORANG SENARAI PERMOHONAN PEMERIKSAAN RADIOLOGI

LOKASI : _____

BIL	KAD PENGENALAN / PASPORT	MRN	NAMA PESAKIT	PEMERIKSAAN	DIAGNOSIS	PRIORITY	TARIKH ORDER	REPORT YA / TIDAK	NAMA DOKTOR	PAKAR AUTHORIZED *UNTUK SPECIAL EXAM

BORANG PENGUJIAN PENERIMAAN PENGGUNA (UAT)
Unit Teknologi Maklumat & Komunikasi (UTMK)
Hospital Tuanku Ja'afar, Seremban

Sila lengkapkan Bahagian A, B dan C. Semua maklumat **WAJIB** diisi.

BAHAGIAN A : MAKLUMAT PENERIMAAN SISTEM APLIKASI UNTUK TUJUAN PENGUJIAN	
NAMA SISTEM APLIKASI:	
JABATAN/UNIT PENERIMA SISTEM APLIKASI:	
TARIKH DAN MASA PENYERAHAN SISTEM APLIKASI KEPADA PENGGUNA UNTUK TUJUAN PENGUJIAN:	
NAMA PEGAWAI PENERIMA SISTEM APLIKASI:	JAWATAN:
	NO. TELEFON:
	E-MEL:

BAHAGIAN B : SENARAI PERMASALAHAN SEMASA FASA PENGUJIAN			
BIL.	MODUL	MASALAH	TINDAKAN UTMK

BAHAGIAN C : PENGESAHAN SERTA PERAKUAN PENERIMAAN DAN PENGUJIAN SISTEM	
TANDATANGAN & COP PEGAWAI PENERIMA	COP RASMI JABATAN/UNIT

BAHAGIAN D : PENGESAHAN UNIT TEKNOLOGI MAKLUMAT & KOMUNIKASI	
TANDATANGAN & COP PEGAWAI UTMK	COP RASMI JABATAN/UNIT

*Sila gunakan lampiran sekiranya ruangan tidak mencukupi.

BORANG PENGUJIAN PENERIMAAN AKHIR (FAT)
Unit Teknologi Maklumat & Komunikasi (UTMK)
Hospital Tuanku Ja'afar, Seremban

Sila lengkapkan Bahagian A dan B. Semua maklumat **WAJIB** diisi.

<table>
<tr><th colspan="2">BAHAGIAN A : MAKLUMAT PENERIMAAN SISTEM APLIKASI</th></tr>
<tr><td colspan="2">NAMA SISTEM APLIKASI:</td></tr>
<tr><td colspan="2">JABATAN/UNIT PENERIMA SISTEM APLIKASI:</td></tr>
<tr><td colspan="2">TARIKH DAN MASA PENYERAHAN SISTEM APLIKASI:</td></tr>
<tr><td rowspan="3">NAMA PEGAWAI PENERIMA SISTEM APLIKASI:</td><td>JAWATAN:</td></tr>
<tr><td>NO. TELEFON:</td></tr>
<tr><td>E-MEL:</td></tr>
<tr><td colspan="2">CATATAN/ ULASAN:</td></tr>
<tr><th colspan="2">BAHAGIAN B : PENGESAHAN SERTA PERAKUAN PENERIMAAN DAN PENGUJIAN SISTEM</th></tr>
<tr><td>TANDATANGAN & COP PEGAWAI PENERIMA</td><td>COP RASMI JABATAN/UNIT</td></tr>
<tr><th colspan="2">BAHAGIAN C : PENGESAHAN UNIT TEKNOLOGI MAKLUMAT & KOMUNIKASI</th></tr>
<tr><td>TANDATANGAN & COP PEGAWAI UTMK</td><td>COP RASMI JABATAN/UNIT</td></tr>
</table>

BORANG PENYERAHAN SISTEM APLIKASI
Unit Teknologi Maklumat & Komunikasi (UTMK)
Hospital Tuanku Ja'afar, Seremban

Sila lengkapkan Bahagian C dan D. Semua maklumat **WAJIB** diisi.

BAHAGIAN A : MAKLUMAT SISTEM APLIKASI
NAMA SISTEM APLIKASI:
FUNGSI SISTEM APLIKASI:
TARIKH PENGUJIAN PENERIMAAN PENGGUNA (UAT):
TARIKH PENGUJIAN PENERIMAAN AKHIR (FAT):

BAHAGIAN B : PERAKUAN PENYERAHAN SISTEM APLIKASI OLEH UTMK

Saya dengan ini mengaku telah menyerahkan sistem aplikasi yang telah dibangunkan oleh saya sepanjang tempoh _____ kepada _____. Sistem tersebut telah diserahkan dalam keadaan berfungsi berdasarkan skop yang telah dipersetujui.

Pembangun Sistem (Seksyen Aplikasi)		Penyelia/ Ketua Unit	
Tandatangan	:	Tandatangan	:
Nama	:	Nama	:
Jawatan	:	Jawatan	:
Tarikh	:	Tarikh	:

BAHAGIAN C : MAKLUMAT PEMILIK SISTEM/ PEGAWAI BERTANGGUNGJAWAB

NAMA	:
JAWATAN	:
JABATAN/UNIT	:
NO. TELEFON	:
E-MEL	:

BAHAGIAN D : PERAKUAN PENERIMAAN SISTEM OLEH JABATAN/ UNIT

Saya dengan ini mengesahkan bahawa jabatan/unit ini telah menerima sistem aplikasi yang dibangunkan oleh UTMK dan akan bertanggungjawab terhadap penggunaan serta pengurusan sistem tersebut.

Tandatangan & Cop Pemilik Sistem
Tarikh:

Cop Rasmi Jabatan/ Unit

BORANG PENAMATAN/PENANGGUHAN SISTEM APLIKASI
Unit Teknologi Maklumat & Komunikasi (UTMK)
Hospital Tuanku Ja'afar, Seremban

Sila lengkapkan Bahagian A dan B. Semua maklumat **WAJIB** diisi.

A. MAKLUMAT PERMOHONAN			
Nama Sistem Aplikasi			
Jabatan/ Unit			
Nama Pemohon		No. Telefon	
Kategori	[ ] Penamatan Tarikh Ditamatkan : _____	[ ] Penangguhan Tarikh Mula Tangguh : _____ Tarikh Guna Semula : _____	
Sebab/Alasan			
Tandatangan dan Cop Pemohon		Tarikh	
B. PENGESAHAN OLEH KETUA JABATAN/UNIT			
Catatan/Ulasan			
Disahkan Oleh (Tandatangan dan Cop)		Cop Rasmi Jabatan/Unit	
		Tarikh	
C. PENGESAHAN UNIT TEKNOLOGI MAKLUMAT & KOMUNIKASI			
Catatan/Ulasan			
Pengesahan UTMK (Tandatangan dan Cop)		Cop Rasmi Jabatan/Unit	
		Tarikh	