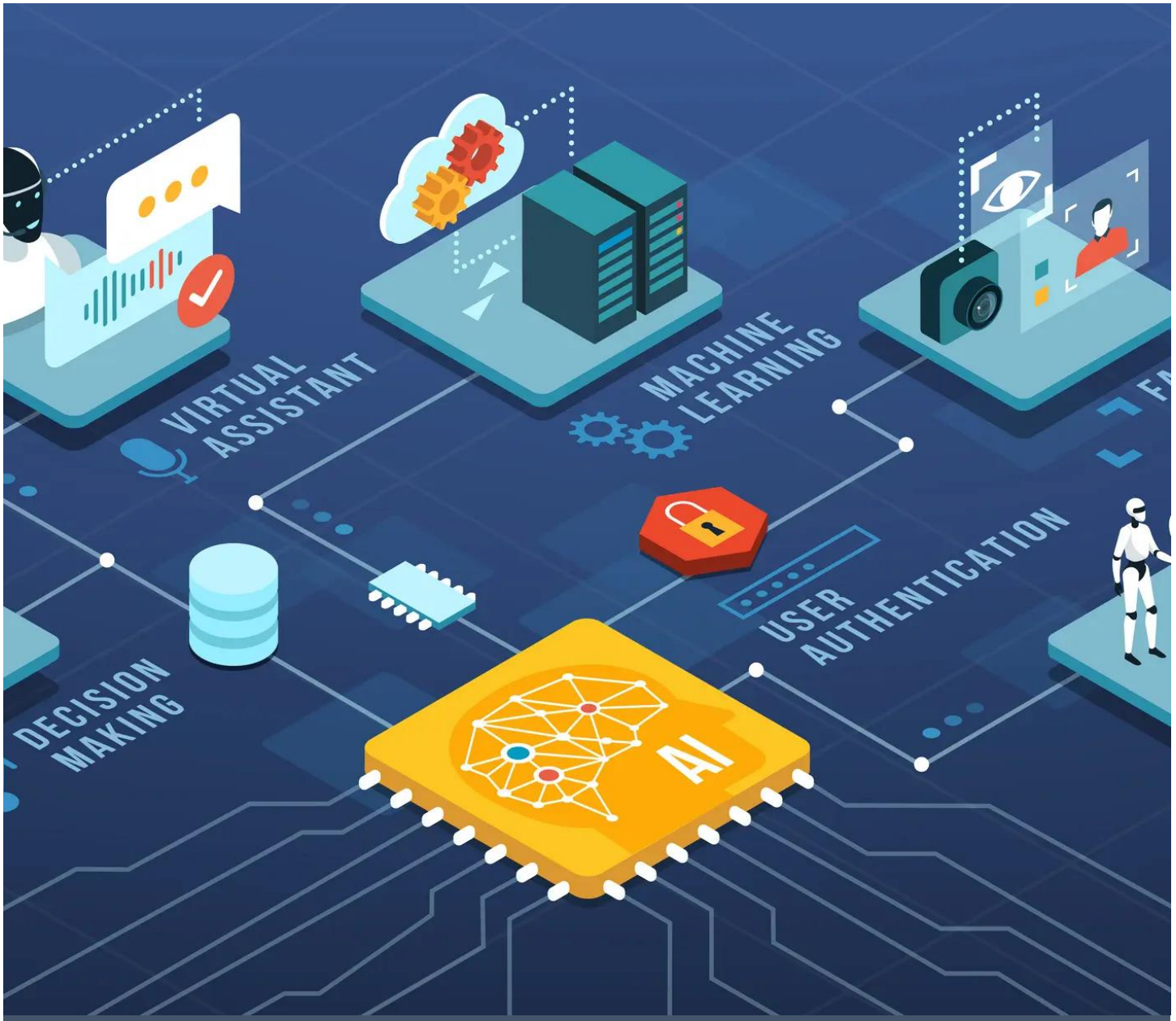

DASAR KESELAMATAN ICT
LEMBAGA ZAKAT NEGERI KEDAH DARUL AMAN
TAHUN 2021

LZNK
LEMBAGA ZAKAT NEGERI KEDAH

REKOD PINDAAN DOKUMEN

NO. KELUARAN	TARIKH KUAT KUASA PINDAAN	BAB / MUKA SURAT		KETERANGAN RINGKAS MENGENAI PINDAAN
01	28-10-2021	Semua	Pindaan keseluruhan dokumen	Pemansuhan DKCIT 2018
02	15-11-2022	Perkara 2 / Mukasurat 14	0201 Infrastruktur Organisasi Dalaman; 2.0 Ketua Pegawai Digital (CDO)	Pemansuhan jawatan Timbalan Ketua Pegawai Eksekutif Pentadbiran dan Kewangan. Ketua Pegawai Teknologi Maklumat di lantik sebagai Ketua Pegawai Digital (CDO).
03	15-11-2022	Lampiran / Mukasurat 92	Surat Akuan Pematuhan Dasar Keselamatan ICT	Tambahan Surat Akuan Pematuhan Dasar Keselamatan ICT meliputi pelajar latihan industri di Lembaga Zakat Negeri Kedah Darul Aman.
04	15-11-2022	Perkara 1 / Mukasurat 11	0101 Dasar Keselamatan ICT; Organisasi Dalaman; 1.0 Pelaksanaan Dasar	Tambahan ahli JPICT: 1. Pakar Teknologi Maklumat Dan Komunikasi

KANDUNGAN

PENDAHULUAN

Lembaga Zakat Negeri Kedah Darul Aman ditubuhkan di bawah Enakmen 23, Enakmen Lembaga Zakat Negeri Kedah Darul Aman 2015 berperanan untuk menyediakan perancangan, pembangunan dan pengurusan bagi perkhidmatan kewangan sosial Islam bertaraf dunia berteraskan profesionalisme, integriti dan teknologi.

Dokumen ini menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dan melindungi aset ICT Lembaga Zakat Negeri Kedah Darul Aman. Dokumen ini diguna pakai oleh semua pihak pegawai, pengguna dan pembekal yang menyediakan perkhidmatan, mencapai dan menggunakan aset dan sistem aplikasi ICT di Lembaga Zakat Negeri Kedah Darul Aman. Penekanan ke atas kesedaran dan tahap keselamatan ICT adalah penting dan perlu diberi perhatian yang serius disebabkan oleh dua faktor.

Faktor pertama ialah keselamatan ICT merupakan tanggungjawab bersama untuk memastikan sistem ICT yang dikendalikan adalah selamat daripada sebarang penyalahgunaan dan ancaman pencerobohan.

Faktor kedua ialah kewujudan penggunaan pebagai teknologi dan platform sistem pengoperasian. Keadaan ini menjadikan ia lebih terbuka kepada ancaman keselamatan. Adalah penting disini supaya penyimpanan maklumat dan penyebaran maklumat perlu dibatasi supaya ia dapat dikawal dengan lebih berkesan.

Dasar Keselamatan ICT (DKICT) Lembaga Zakat Negeri Kedah Darul Aman mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT Lembaga Zakat Negeri Kedah Aman.

VISI

Mewujudkan persekitaran sistem ICT yang komprehensif, selamat, berkesan, stabil dan boleh dipercayai (*reliable).*

MISI

Untuk mencapai tahap keselamatan ICT yang menyeluruh bagi menyokong peranan Lembaga Zakat Negeri Kedah Darul Aman dalam melindungi kepentingan strategik dan aset-asetnya.

OBJEKTIF

DKICT Lembaga Zakat Negeri Kedah Darul Aman diwujudkan untuk menjamin kesinambungan urusan Lembaga Zakat Negeri Kedah Darul Aman dengan meminimumkan kesan insiden keselamatan ICT.

Dasar ini juga sesuai untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi Lembaga Zakat Negeri Kedah Darul Aman. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi. Manakala objektif utama DKICT di Lembaga Zakat Negeri Kedah Darul Aman adalah seperti berikut:

i. Memastikan kelancaran operasi Lembaga Zakat Negeri Kedah Darul Aman yang berlandaskan ICT dengan mencegah serta meminimumkan kerosakan atau kemusnahan aset ICT Lembaga Zakat Negeri Kedah Darul Aman;
ii. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan maklumat dan komunikasi;
iii. Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;
iv. Meningkatkan tahap kesedaran keselamatan ICT kepada para pegawai, pengguna dan pembekal;
v. Memperkemaskan pengurusan risiko;
vi. Melindungi kepentingan aset-aset dan pihak-pihak yang bergantung kepada sistem dan sumber ICT Lembaga Zakat Negeri Kedah Darul Aman daripada kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi.
vii. Mencegah penyalahgunaan atau kecurian aset ICT Lembaga Zakat Negeri Kedah Darul Aman; dan
viii. Melindungi aset ICT daripada penyelewengan oleh pegawai, pengguna dan pembekal.

SKOP

Aset ICT Lembaga Zakat Negeri Kedah Darul Aman terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan sumber manusia. DKICT Lembaga Zakat Negeri Kedah Darul Aman menetapkan keperluan-keperluan asas berikut:

a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan

b) Semua data dan maklumat hendaklah dijaga kerahsiannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan Lembaga Zakat Negeri Kedah Darul Aman, perkhidmatan dan orang awam.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, DKICT Lembaga Zakat Negeri Kedah Darul Aman ini merangkumi perlindungan semua bentuk maklumat yang dimasukkan, diwujudkan, dimusnahkan, disimpan, dijana, dicetak, diakses, diedar dalam penghantaran dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

a) Perkakasan

Aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan Lembaga Zakat Negeri Kedah Darul Aman. Contoh komputer, *server*, peralatan komunikasi dan sebagainya;

b) Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian sistem pangkalan data perisian sistem rangkaian atau aplikasi gunasama yang menyediakan kemudahan pemprosesan maklumat kepada Lembaga Zakat Negeri Kedah Darul Aman;

c) Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi- fungsinya. Contoh:

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

d) Data atau maklumat

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif Lembaga Zakat Negeri Kedah Darul Aman. Contohnya sistem dokumentasi, standard operasi prosedur, rekod-rekod rasmi, profil-profil pelanggan, pangkalan data dan fail-fail data serta maklumat-maklumat arkib dan lain-lain;

e) Manusia

Semua pengguna infrastruktur Lembaga Zakat Negeri Kedah Darul Aman yang dibenarkan, termasuk pegawai, pengguna dan pembekal. Individu yang mempunyai pengetahuan untuk melaksanakan skop kerja harian Lembaga Zakat Negeri Kedah Darul Aman bagi mencapai misi dan objektif Lembaga Zakat Negeri Kedah Darul Aman. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan;

f) Dokumentasi

Semua dokumen (prosedur dan manual pengguna) yang berkaitan dengan aset ICT, pemasangan dan pengoperasian peralatan dan perisian, sama ada dalam bentuk elektronik atau bukan elektronik;

g) Premis Komputer dan Komunikasi

Semua kemudahan serta premis yang diguna untuk menempatkan perkara a) – f) di atas. Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

PERNYATAAN DASAR

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

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat komponen asas keselamatan ICT iaitu:

i. Melindungi maklumat rahsia rasmi dan maklumat rasmi Lembaga Zakat Negeri Kedah Darul Aman dari capaian tanpa kuasa yang sah;
ii. Menjamin setiap maklumat adalah tepat dan sempurna;
iii. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna;
iv. Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

DKICT Lembaga Zakat Negeri Kedah Darul Aman merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

i. **Kerahsiaan** - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
ii. **Integriti** - Data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan;
iii. **Tidak Boleh Disangkal** - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
iv. **Kesahihan** - Data dan maklumat hendaklah dijamin kesahihannya;
v. **Ketersediaan** - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT Lembaga Zakat Negeri Kedah Darul Aman dan perlu dipatuhi adalah seperti berikut:

a) Akses Atas Dasar Perlu Mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu mengikut dasar perlu mengetahui sahaja. Pertimbangan akses di bawah prinsip ini hendaklah berteraskan kepada klasifikasi maklumat dan tapisan keselamatan yang dihadkan kepada pengguna.

Klasifikasi maklumat hendaklah mematuhi ”Arahan Keselamatan Kerajaan”. Maklumat ini dikategorikan kepada Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka. Penggunaan *encryption*, tandatangan digital atau sebarang mekanisma lain yang boleh melindungi maklumat mestilah juga dipertimbangkan. Dasar klasifikasi ke atas sistem aplikasi juga hendaklah mengikut klasifikasi maklumat yang sama;

b) Hak Akses Minimum

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

c) Akauntabiliti / Intergriti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mempunyai keupayaan mengesan dan mengesahkan pengguna boleh dipertanggungjawabkan atas tindakan mereka.

Data dan maklumat hendaklah tepat, lengkap dan sentiasa terkini. Sebarang perubahan terhadap data hendaklah dilaksanakan oleh pegawai yang diberi kebenaran sahaja.

Akauntabiliti atau tanggungjawab pengguna merangkumi perkara berikut:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
iii. Menjaga kerahsiaan kata laluan;
iv. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
v. Memberi perhatian kepada maklumat terperingkat terutama semasa pengwujudan, pemprosesan, penyimpanan, penyelenggaraan, penghantaran, penyampaian, pertukaran dan pemusnahan.

d) Pengauditan Keselamatan

Pengauditan adalah tindakan untuk mengenalpasti insiden berkaitan keselamatan atau mengenalpasti keadaan yang mengancam keselamatan ICT. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

Pentadbir Sistem perlu memastikan semua log / audit *trail* yang dijanakan oleh aset ICT berkaitan keselamatan disimpan sekurang-kurangnya 1 tahun bagi tujuan jejak audit. Rekod audit hendaklah dilindungi dan tersedia untuk penilaian apabila diperlukan. Ketua Divisyen Teknologi Maklumat perlu mempertimbangkan penggunaan perisian tambahan bagi menentukan ketepatan dan kesahihan log / audit *trail*;

e) Pemulihan

Pemulihan sistem ICT amat diperlukan untuk memastikan kebolehsediaan, kebolehcapaian dan kerahsiaan. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan.

Pemulihan hendaklah dilakukan melalui tindakan berikut:

i. Pelan Pemulihan Bencana Sistem ICT hendaklah diuji sekurang-kurangnya sekali setahun. Ketua Divisyen Teknologi Maklumat dikehendaki menentukan perkara ini dilaksanakan.
ii. Pemulihan boleh dilakukan melalui proses penduaan (*backup*) dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan (BRP). Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian bagi meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan dan ketidakbolehcapaian;

f) Pematuhan

Pematuhan DKICT Lembaga Zakat Negeri Kedah Darul Aman adalah berdasarkan tindakan berikut:

i. Mewujudkan proses yang sistematik khususnya untuk menjamin keselamatan ICT bagi memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan
ii. Merumus pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenalpasti.
iii. Pelaksanaan program pengawasan dan pemantauan keselamatan maklumat secara berterusan hendaklah dilaksanakan. Divisyen Keselamatan Siber Dan Perkhidmatan Pengguna ICT berperanan melaksanakan pengawasan dan pemantauan menyeluruh terhadap keselamatan maklumat pada aset-aset ICT di Lembaga Zakat Negeri Kedah Darul Aman.
iv. Menguatkuasakan amalan melapor sebarang insiden yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan / pemulihan;

g) Pengasingan

Tugas mewujud, menghapus, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan (*unauthorized access*) serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan juga merangkumi tindakan memisahkan antara Pentadbir Sistem dan Pentadbir Rangkaian Dan Keselamatan. Pengasingan fungsi perlu diadakan di antara pentadbir dan pengguna.

h) Autentikasi

Proses ini merupakan keupayaan bagi membuktikan bahawa sesuatu mesej atau maklumat tertentu telah dihantar oleh pemilik asal yang dikenalpasti. Setiap sistem ICT berangkaian hendaklah dilengkapi dengan sistem autentikasi yang secukupnya. Bagi sistem yang mengendalikan maklumat terperingkat, ciri penyahsangkalan hendaklah digunakan;

i) Perimeter Keselamatan Fizikal

Perimeter merujuk kepada keadaan persekitaran fizikal di mana aset-aset ICT dilindungi. Perimeter tersebut hendaklah dijaga dengan rapi bagi mengelakkan sebarang pencerobohan. Ketua Divisyen Keselamtan Siber Dan Perkhidmatan Pengguna ICT hendaklah memastikan proses ini laksanakan;

h) Pertahanan Berlapis (*Defense in Depth*)

Pertahanan berlapis hendaklah diwujudkan untuk melindungi keselamatan aset ICT dari pencerobohan. Ketua Divisyen Keselamatan Siber Dan Perkhidmatan Pengguna ICT hendaklah menentukan sistem ICT mempunyai pertahanan berlapis yang lengkap mengikut teknologi semasa; dan

i) Saling Bergantung

Langkah-langkah keselamatan ICT yang berkesan memerlukan pematuhan kepada semua prinsip-prinsip tersebut. Setiap prinsip adalah saling lengkap-melengkapi antara satu dengan yang lain. Tindakan mempersepadukan prinsip yang telah dinyatakan perlu dilaksanakan bagi menjamin tahap keselamatan yang maksimum.

PENILAIAN RISIKO KESELAMATAN ICT

Divisyen Keselamatan Siber Dan Perkhidmatan Pengguna ICT hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu, ia perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

Divisyen Keselamatan Siber Dan Perkhidmatan Pengguna ICT hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat Lembaga Zakat Negeri Kedah Darul Aman termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik stor penyimpanan peralatan ICT, kemudahan utiliti dan sistem-sistem sokongan lain.

Divisyen Keselamatan Siber Dan Perkhidmatan Pengguna ICT bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

Divisyen Keselamatan Siber Dan Perkhidmatan Pengguna ICT perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

1. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
2. Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh Lembaga Zakat Negeri Kedah Darul Aman;
3. Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko;
4. Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

PERKARA 01: PEMBANGUNAN DAN PENYELENGGARAAN DASAR

0101 DASAR KESELAMATAN ICT		
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan Lembaga Zakat Negeri Kedah Darul Aman dan perundangan yang berkaitan.		
1.0	**Pelaksanaan Dasar**	
	Pelaksanaan Dasar ini dijalankan oleh Ketua Pegawai Eksekutif dibantu oleh Jawatankuasa Pemandu ICT Lembaga Zakat Negeri Kedah Darul Aman (JPICT) yang terdiri daripada: i) Ketua Pegawai Digital (CDO); ii) Pegawai Keselamatan ICT (ICTSO); iii) Pengurus ICT; iv) Ketua Divisyen; v) Pegawai Zakat Daerah; dan / atau vi) Pakar Teknologi Maklumat Dan Komunikasi.	Ketua Pegawai Eksekutif
2.0	**Penyebaran Dasar**	
	Dasar ini perlu disebarkan kepada semua pengguna Lembaga Zakat Negeri Kedah Darul Aman termasuk pegawai,pengguna, pembekal dan lain-lain.	ICTSO
3.0	**Penyelenggaraan Dasar**	
	DKICT Lembaga Zakat Negeri Kedah Darul Aman ini adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan DKICT: i. Kenalpasti dan tentukan perubahan yang diperlukan; ii. Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk dibentangkan kepada Jawatankuasa Pemandu ICT bagi mendapatkan persetujuan Jawatankuasa Pemandu ICT Lembaga Zakat Negeri Kedah Darul Aman; iii. Perubahan yang telah dipersetujui oleh Jawatankuasa Pemandu ICT Lembaga Zakat Negeri Kedah Darul Aman diserahkan kepada Jawatankuasa Pengurusan Tertinggi untuk semakan dan di makluman kepada Mesyuarat Ahli Lembaga Zakat Negeri Kedah Darul Aman untuk kelulusan; iv. Perubahan yang telah diluluskan oleh Mesyuarat Ahli Lembaga Zakat Negeri Kedah Darul Aman hendaklah dimaklumkan kepada pegawai, pengguna dan pembekal; dan v. Menyemak semula dokumen pada jangka masa yang dirancang atau mengikut keperluan dan perubahan ketara bagi memastikan dokumen sentiasa relevan dan berkesan;	JPICT; ICTSO

4.0	**Pengecualian Dasar**	
	DKICT Lembaga Zakat Negeri Kedah Darul Aman adalah terpakai dan mestilah dipatuhi oleh semua pegawai, pengguna serta pembekal ICT Lembaga Zakat Negeri Kedah Darul Aman dan tiada pengecualian diberikan.	Semua

PERKARA 02: ORGANISASI PENGURUSAN KESELAMATAN ICT

0201 INFRASTRUKTUR ORGANISASI DALAMAN		
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi		
1.0	**Ketua Pegawai Esekutif**	
	Peranan dan tanggungjawab adalah seperti berikut: i. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah DKICT Lembaga Zakat Negeri Kedah Darul Aman; ii. Memastikan semua pengguna mematuhi DKICT Lembaga Zakat Negeri Kedah Darul Aman; iii. Memastikan semua keperluan organisasi sumber kewangan, sumber pegawai dan perlindungan keselamatan adalah mencukupi.	Ketua Pegawai Ekeskutif
2.0	**Ketua Pegawai Digital (CDO)**	
	Ketua Pegawai Digital (CDO) bagi Lembaga Zakat Negeri Kedah Darul Aman adalah Ketua Pegawai Teknologi Maklumat. Peranan dan tanggungjawab CDO adalah seperti berikut: i. Membantu Ketua Pegawai Esekutif dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; ii. Menentukan keperluan keselamatan ICT; iii. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT Lembaga Zakat Negeri Kedah Darul Aman; iv. Memastikan setiap pegawai menandatangani Surat Akuan Mematuhi DKICT Lembaga Zakat Negeri Kedah Darul Aman; dan v. Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT Lembaga Zakat Negeri Kedah Darul Aman.	CDO
3.0	**Pegawai Keselamatan ICT (ICTSO)**	
	Peranan dan tanggungjawab Pegawai Keselamatan ICT adalah seperti berikut: i. Mengurus keseluruhan program-program keselamatan ICT; ii. Menguatkuasakan pelaksanaan DKICT Lembaga Zakat Negeri Kedah Darul Aman; iii. Memberi penerangan dan pendedahan berkenaan DKICT Lembaga Zakat Negeri Kedah Darul Aman kepada semua pengguna; iv. Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT;	ICTSO

	v. Menentukan tahap keutamaan insiden ICT dan melaporkan insiden keselamatan ICT kepada CDO bagi mengambil langkah pemulihan awal dan membuat makluman didalam Mesyuarat Jawatankuasa Pemandu ICT; vi. Melaporkan insiden keselamatan ICT kepada pihak *National Cyber Security Agency* (NACSA) dan CyberSecurity Malaysia (jika perlu) dan seterusnya membantu dalam penyiasatan atau pemulihan; vii. Bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan mengesyorkan langkah-langkah baik pulih dengan segera; viii. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan; ix. Mengesyorkan proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar DKICT Lembaga Zakat Negeri Kedah Darul Aman kepada Jawantankuasa Tatatertib Lembaga Zakat Negeri Kedah Darul Aman; x. Melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT *Security Posture Assessment* (SPA) serta penilaian risiko keselamatan maklumat; xi. Penyelaras Pengurusan Kesinambungan Perkhidmatan ICT Lembaga Zakat Negeri Kedah Darul Aman; dan xii. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT Lembaga Zakat Negeri Kedah Darul Aman.	
4.0	**Pengurus ICT**	
	Pengurus ICT bagi Lembaga Zakat Negeri Kedah Darul Aman ialah Ketua Divisyen yang ditempatkan dibawah pentadbiran Pejabat Ketua Pegawai Teknologi Maklumat kecuali ICTSO Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: i. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan Lembaga Zakat Zakat Negeri Kedah Darul Aman; ii. Menjalankan pengurusan risiko; iii. Menentukan kawalan akses pengguna terhadap aset ICT Lembaga Zakat Negeri Kedah Darul Aman; iv. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT;	Pengurus ICT

	v. Mengkaji semula aspek-aspek keselamatan fizikal seperti kemudahan *backup* dan persekitaran pejabat yang perlu; vi. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; vii. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Lembaga Zakat Negeri Kedah Darul Aman. viii. Melaksanakan keperluan DKICT dalam operasi semasa seperti berikut: i) Pelaksanaan sistem atau aplikasi baru sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baru; ii) Pembelian atau peningkatan perisian dan sistem komputer; iii) Perolehan teknologi dan perkhidmatan komunikasi baru; ix. Membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi mematuhi keperluan DKICT Lembaga Zakat Negeri Kedah Darul Aman; dan x. Membangun mengkaji semula dan mengemas kini pelan kontingensi keselamatan ICT.	
5.0	**Pentadbir Sistem ICT**	
	Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: i. Memastikan ketepatan dan menyekat kebenaran capaian serta-merta apabila tidak lagi diperlukan atau melanggar DKICT Lembaga Zakat Negeri Kedah Darul Aman; ii. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pegawai yang telah tamat perkhidmatan, bertukar, berhenti atau berlaku perubahan dalam bidang tugas; iii. Melaksanakan prinsip-prinsip DKICT dan menjaga kerahsiaan maklumat Lembaga Zakat Negeri Kedah Darul Aman; iv. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT Lembaga Zakat Negeri Kedah Darul Aman; v. Memantau aktiviti capaian sistem aplikasi pengguna; vi. Menyediakan laporan mengenai aktiviti capaian secara berkala. vii. Menganalisa dan menyimpan rekod jejak audit; viii. Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;	Pentadbir Sistem

6.0	**Pentadbir Rangkaian Dan Keselamatan**	
	Peranan dan tanggungjawab Pentadbir Rangkaian Dan Keselamatan adalah seperti berikut: i. Memastikan LAN dan WAN di Lembaga Zakat Negeri Kedah Darul Aman beroperasi sepanjang masa; ii. Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; iii. Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; iv. Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian Lembaga Zakat Negeri Kedah Darul Aman secara tidak sah; v. Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; dan vi. Memastikan maklumat perhubungan perlu dikemaskini dari semasa ke semasa.	Pentadbir Rangkaian Dan Keselamatan
7.0	**Pentadbir Portal Dan Media Sosial**	
	Peranan dan tanggungjawab Pentadbir Portal Dan Media Sosial adalah seperti berikut: i. Memastikan kandungan sentiasa sahih dan terkini daripada sumber yang sah; ii. Memantau capaian portal dan menjalankan penilaian prestasi untuk memastikan akses yang lancar; iii. Prihatin terhadap peraturan atau syarat-syarat yang digariskan oleh penyedia platform media sosial; iv. Menegur *posting* atau komen untuk memastikan perbincangan berada di landasan yang betul; v. Sentiasa semak posting atau komen (dengan seorang moderator, jika boleh); vi. Mempertimbangkan untuk mengeluarkan atau menyekat mereka yang terus membuat *posting* atau komen jelik;	Pentadbir Portal Dan Media Sosial

	vii. Mengasingkan kandungan dan aplikasi dalam talian untuk capaian secara Intranet dan Internet ke portal; viii. Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai antara muka portal; ix. Memastikan hanya maklumat yang bersifat terbuka dipaparkan di portal dan media sosial; x. Memastikan reka bentuk portal dibangunkan dengan ciri-ciri keselamatan supaya tidak diceroboh; xi. Memastikan data-data SULIT tidak boleh disalin atau dicetak oleh orang yang tidak berhak; xii. Melaksanakan proses *backup* dan *restoration* ke atas kandungan dan aplikasi portal; dan xiii. Melaporkan sebarang pelanggaran polisi penggunaan dan keselamatan yang sedang berkuatkuasa kepada ICTSO;	
8.0	**Pengguna**	
	Pengguna terdiri daripada warga Lembaga Zakat Negeri Kedah Darul Aman dan pihak luaran yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Lembaga Zakat Negeri Kedah Darul Aman. Peranan dan tanggungjawab pengguna adalah seperti berikut: i. Pengguna perlu membaca, memahami dan mematuhi DKICT Lembaga Zakat Negeri Kedah Darul Aman; ii. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; iii. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; iv. Melaksanakan prinsip-prinsip DKICT Lembaga Zakat Negeri Kedah Darul Aman dan menjaga kerahsiaan maklumat Lembaga Zakat Negeri Kedah Darul Aman; v. Melaksanakan langkah-langkah perlindungan seperti berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata nama dan kata laluan; v. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan;	Semua

	vi. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. vi. Melaksanakan prinsip-prinsip DKICT Lembaga Zakat Negeri Kedah Darul Aman dan menjaga kerahsiaan maklumat Lembaga Zakat Negeri Kedah Darul Aman; vii. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan viii. Mengawal aktiviti penggunaan media sosial seperti di bawah: i. Mengelakkan ketirisan maklumat; ii. Tidak memberi atau mendedahkan sebarang komen atau pernyataan atau isu yang menyentuh perkara-perkara boleh menyebabkan imej dan dasar Lembaga Zakat Negeri Kedah Darul Aman; iii. Tidak menyebarkan maklumat yang berbentuk fitnah, hasutan dan lucah atau cuba memprovokasikan sesuatu isu yang menyalahi peraturan dan undang-undang atau perkara yang menyentuh sensitiviti individu atau kumpulan tertentu; dan iv. Tidak menggunakan saluran media sosial hingga mengganggu fokus dalam urusan kerja. i. Menandatangani Surat Akuan Pematuhan DKICT Lembaga Zakat Negeri Kedah Darul Aman.	

9.0	**Jawatankuasa Pemandu ICT (JPICT)**	
	Keanggotaan JPICT adalah seperti berikut: Pengerusi: CDO Ahli: i. ICTSO; ii. Pengurus ICT; iii. Ketua Divisyen; iii. Pegawai Zakat Daerah; dan / atau iv. Pakar Teknologi Maklumat Dan Komunikasi Urusetia: Divisyen Teknologi Maklumat Bidang kuasa: i. Meneliti, meluluskan dan menguatkuasakan DKICT; ii. Menetapkan arah tuju dan strategi ICT untuk pelaksanaan ICT Lembaga Zakat Negeri Kedah Darul Aman; iii. Merancang, menyelaras dan memantau pelaksanaan program atau projek ICT agar selari dengan Pelan Strategik Lembaga Zakat Negeri Kedah Darul Aman; iv. Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju/strategi ICT Lembaga Zakat Negeri Kedah Darul Aman; v. Merancang dan menentukan langkah-langkah keselamatan ICT; vi. Meluluskan tahap pematuhan keselamatan ICT; vii. Meneliti dan meluluskan semua program dan aktiviti yang berkaitan dengan keselamatan ICT; viii. Merancang dan meluluskan skop pensijilan ISMS; ix. Meluluskan projek-projek ICT; x. Mengikuti dan memantau perkembangan program ICT serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT; xi. Memantau ancaman-ancaman utama terhadap aset-aset ICT; xii. Mengemukakan laporan kemajuan projek ICT yang diluluskan; dan xiii. Memastikan pengauditan sistem ICT dilaksanakan sekurang-kurangnya sekali setahun.	JPICT

10.0	**Pasukan Tindak Balas Insiden Keselamatan ICT Dan Pelan Pemulihan Bencana (CERT& DRP)**	
	Keanggotaan CERT & DRP adalah seperti berikut: Pengerusi: CDO Setiausaha: ICTSO Ahli: i. Pengurus ICT; ii. Ketua Unit; iii. Pegawai di turunkan kuasa; dan / atau iv. Pakar Teknologi Maklumat; dan v. Pembekal (jika berkenaan). Urusetia: Divisyen Keselamatan Siber Dan Perkhidmatan Pengguna ICT Bidang kuasa: i. Membangunkan Dokumen Pelan Pemulihan Bencana (DRP); ii. Menyediakan kemudahan pemulihan bencana atau Pusat Pemulihan Bencana (*Disaster Recovery Centre*); iii. Membuat penilaian ke atas masalah dan jangkaan akibat bencana; iv. Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden; v. Merekod dan menjalankan siasatan awal insiden yang diterima; vi. Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; vii. Memaklumkan CDO berkenaan bencana, kemajuan pemulihan bencana dan masalah; viii. Menghubungi dan melaporkan insiden yang berlaku kepada CTO dan pihak *National Cyber Security Agency* (NACSA) dan CyberSecurity Malaysia (jika perlu) sama ada sebagai *input* atau untuk tindakan seterusnya; ix. Mengaktifkan prosedur pemulihan bencana; x. Mengkoordinasi operasi pemulihan; xi. Menjalankan dan memantau operasi pemulihan; xii. Mendokumentasikan operasi pemulihan; xiii. Mengkoordinasi simulasi pemulihan bencana; dan xiv. Melaporkan sebarang maklumbalas dan insiden keselamatan ICT kepada JPICT.	CERT & DRP

0202 PIHAK LUARAN

Objektif:
Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain)

1.0	**Keperluan Keselamatan Dalam Perkhidmatan ICT**	
	Pihak Luaran terdiri daripada pembekal, pakar runding, penyewa dan pihak-pihak lain yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT atau pelawat yang mengunjungi Lembaga Zakat Negeri Kedah Darul Aman atas urusan rasmi. Perkara yang perlu dipatuhi: i. Mengenal pasti risiko ke atas keselamatan maklumat dan memastikan pelaksanaan kawalan yang sesuai ke atas maklumat tersebut; ii. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga; iii. Akses kepada aset ICT Lembaga Zakat Negeri Kedah Darul Aman perlu berlandaskan perjanjian dan peraturan yang telah ditetapkan. Perjanjian yang dimeterai perlu mematuhi perkara-perkara berikut: i. DKICT Lembaga Zakat Negeri Kedah Darul Aman; ii. Tapisan Keselamatan iii. Arahan Teknologi Maklumat 2007 (*IT Instructions*); iv. Perakuan Akta Rahsia Rasmi 1972; dan v. Hak Harta Intelek. iv. Lulus tapisan keselamatan dan menandatangani Surat Akuan Pematuhan DKICT Lembaga Zakat Negeri Kedah Darul Aman serta Perakuan Akta Rahsia Rasmi 1972 bagi perakuan untuk tidak membocorkan sebarang maklumat rasmi yang diperolehi sepanjang berkhidmat dengan Lembaga Zakat Negeri Kedah Darul Aman; dan v. Pihak luaran kategori pelawat sahaja dikecualikan daripada mematuhi peraturan i. hingga iv. seperti di atas.	Semua

PERKARA 03: KESELAMATAN SUMBER MANUSIA

Keperluan Keselamatan Dalam Perkhidmatan ICT		
Objektif: Memastikan semua pengguna yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.		
1.0	**Sebelum Perkhidmatan**	
	Memastikan semua pengguna yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, penipuan dan penyalahgunaan aset ICT. Perkara yang mesti dipatuhi termasuk yang berikut: i. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab semua pengguna yang berkepentingan ke atas keselamatan ICT sebelum, semasa dan selepas perkhidmatan; ii. Lulus tapisan keselamatan dan menandatangani Surat Akuan Pematuhan DKICT Lembaga Zakat Negeri Kedah Darul Aman untuk semua pengguna; iii. Memastikan pihak luaran menandatangani Surat Akuan Pematuhan DKICT Lembaga Zakat Negeri Kedah Darul Aman, lulus Tapisan Keselamatan dan Perakuan Akta Rahsia Rasmi 1972; dan iv. Mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua
2.0	**Semasa Perkhidmatan**	
	Memastikan semua pengguna yang berkepentingan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong DKICT Lembaga Zakat Negeri Kedah Darul Aman dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara yang mesti dipatuhi termasuk yang berikut: i. Memastikan semua pengguna yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan ditetapkan Lembaga Zakat Negeri Kedah Darul Aman; ii. Memastikan latihan dan program kesedaran yang berkaitan keselamatan ICT diberikan kepada pengguna dari semasa ke semasa;	Semua

	iii. Memastikan prosedur latihan sentiasa dikemas kini bersesuaian dengan fungsi tugas semasa setiap pengguna; iv. Memastikan adanya tindakan tatatertib/ atau perundangan ke atas semua pengguna sekiranya berlaku pelanggaran keselamatan maklumat; dan v. Memantapkan pengetahuan berkaitan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.	
3.0	**Bertukar Atau Tamat Perkhidmatan**	
	Memastikan pertukaran atau tamat perkhidmatan semua pengguna yang berkepentingan diuruskan dengan teratur. Perkara yang mesti dipatuhi termasuk yang berikut: i. Memastikan semua aset ICT dikembalikan kepada Lembaga Zakat Negeri Kedah Darul Aman mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan ii. Membatalkan atau meminda semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan Lembaga Zakat Negeri Kedah Darul Aman dan/atau terma perkhidmatan.	Semua

PERKARA 04: PENGURUSAN ASET

Keperluan Keselamatan Dalam Perkhidmatan ICT		
Objektif: Memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT Lembaga Zakat Negeri Kedah Darul Aman.		
0401 Akauntabiliti Aset ICT		
Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT Lembaga Zakat Negeri Kedah Darul Aman.		
	Tanggungjawab yang perlu dipatuhi untuk memastikan semua aset ICT dikawal dan dilindungi: i. Memastikan semua aset ICT dikenal pasti, dikelas, didokumen, diselenggara dan dilupuskan; ii. Maklumat aset direkod dan dikemas kini dalam Sistem Pengurusan Aset Alih mengikut Tatacara Pengurusan Aset Alih yang berkuatkuasa dan sentiasa dikemaskini; iii. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; iv. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di Lembaga Zakat Negeri Kedah Darul Aman; v. Memastikan semua peraturan pengendalian aset ICT dikenal pasti, didokumen dan dilaksanakan; vi. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; vii. Penggunaan aset ICT Lembaga Zakat Negeri Kedah Darul Aman mestilah tujuan tugas rasmi sahaja; dan viii. Sebarang perlanggaran hendaklah dilaporkan kepada CDO.	Pegawai Aset; Semua
0402 Pengelasan dan Pengendalian Maklumat		
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.		
1.0	**Pengelasan Maklumat**	
	Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada Lembaga Zakat Negeri Kedah Darul Aman. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan seperti berikut: i. Rahsia Besar; ii. Rahsia; iii. Sulit; atau iv. Terhad. v. Terbuka.	Semua

2.0	**Pengendalian Maklumat**	
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai,menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut; i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan; vi. Melaksanakan peraturan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum; dan viii. Mewujudkan salinan pendua maklumat penting bagi mengurangkan risiko kehilangan dan kemusnahan.	Semua
0403 Data Terbuka Lembaga Zakat Negeri Kedah Darul Aman		
Objektif: Memudahkan capaian kepada data dan maklumat milik Lembaga Zakat Negeri Kedah Darul Aman yang boleh dikongsi dalam bentuk kebolehbacaan mesin dan kebolehbacaan manusia dengan cara yang proaktif. Perkongsian dan capaian akan dilaksanakan di dalam kerangka dasar-dasar, akta dan peraturan yang berkaitan, dengan itu membenarkan capaian dan penggunaan data dan maklumat Lembaga Zakat Negeri Kedah Darul Aman secara lebih meluas melalui penerbitan data tebuka untuk kegunaan awam.		
	Data terbuka merujuk kepada data Lembaga Zakat Negeri Kedah Darul Aman yang boleh digunakan secara bebas, boleh dikongsikan dan digunakan semula oleh orang awam, agensi sektor awam atau swasta untuk sebarang tujuan. Pelaksanaan data terbuka dapat meningkatkan imej, kualiti, ketelusan dan kepercayaan pengurusan Lembaga Zakat Negeri Kedah Darul Aman menerusi perkongsian data yang tepat, cepat dan relevan. Di samping itu, ia juga dapat meningkatkan peningkatan kutipan akat dan agihan zakat di negeri Kedah Darul Aman. Data Terbuka adalah maklumat yang bebas digunakan, dikongsi dan digunakan semula oleh orang awam, agensi sektor awam dan organisasi swasta untuk pelbagai tujuan.	Semua

PERKARA 05: KAWALAN CAPAIAN

Dasar Kawalan Capaian		
Objektif: Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT.		
0501 Kawalan Capaian		
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	Pentadbir Sistem
0502 Pengurusan Capaian Pengguna		
1.0	**Pendaftaran Pengguna**	
	Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, Pentadbir Sistem perlu mengambil langkah-langkah berikut: i. Akaun yang diperuntukkan oleh Lembaga Zakat Negeri Kedah Darul Aman sahaja boleh digunakan; ii. Akaun kata nama hendaklah mencerminkan identiti pengguna; iii. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan Lembaga Zakat Negeri Kedah Darul Aman. Akaun boleh ditarik balik jika kaedah penggunaannya melanggar peraturan; iv. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan v. Pentadbir Sistem boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Pengguna bercuti panjang dalam tempoh waktu melebihi enam (6) bulan; ii. Bertukar bidang tugas kerja; iv. Berhenti atau iv. Ditamatkan perkhidmatan.	Pentadbir Sistem; Semua
2.0	**Hak Capaian (*Privilege*)**	
	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pemilik Sistem, Pentadbir Sistem

3.0	**Semakan Hak Capaian Pengguna**	
	Pemilik sistem perlu menyemak hak capaian pengguna dari masa ke semasa bagi memastikan tiada berlaku penyalahgunaan hak capaian.	Pemilik Sistem, Pentadbir Sistem
4.0	**Pengurusan Kata Laluan**	
	Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh Lembaga Zakat Negeri Kedah Darul Aman seperti berikut: i. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; ii. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; iii. Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf, nombor (alphanumerik), karakter istimewa (contoh @, $, #) dan perlu mengandungi gabungan huruf besar dan kecil; iv. Kata laluan hendaklah diingat dan tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun; v. Kata laluan sistem pengoperasian atau *Active Directory* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama; vi. Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; vii. Kuatkuasakan pertukaran kata laluan semasa log masuk kali pertama atau selepas log masuk kali pertama atau selepas kata laluan diset semula; viii. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; ix. Had kemasukan katalaluan bagi capaian kepada sistem aplikasi adalah maksimum tiga (3) kali sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga kata nama capaian diaktifkan semula; x. Kata laluan hendaklah disimpan dalam bentuk yang telah dienkripkan; xi. Kata laluan disarankan untuk ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; xii. Mengelakkan penggunaan semula kata laluan yang telah digunakan; xiii. Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna; dan xiv. Penggunaan *default administrator* dan *guest* adalah tidak dibenarkan.	Pentadbir Sistem; Semua

0503 Tanggungjawab Pengguna		
Objektif: Menghalang capaian yang tidak dibenarkan terhadap maklumat dan fasiliti pemprosesan.		
1.0	**Penggunaan Akaun Dan Kata Laluan**	
	Capaian kepada sistem ICT Lembaga Zakat Negeri Kedah Darul Aman perlu mempunyai akaun pengenalan diri dan kata laluan. Antara perkara yang perlu dipatuhi ialah: i. Penggunaan akaun *administrator* adalah dilarang; ii. *System administrator* yang dilantik perlu menggunakan akaun sendiri tetapi mempunyai capaian sebagai *administrator* kecuali di dalam keadaan yang tertentu; iii. Salinan akaun dan kata laluan *administrator* hendaklah disimpan oleh ICTSO dan jika berlaku pertukaran katalaluan, salinan tersebut perlu dikemaskini; iv. Pengguna tidak dibenarkan menggunakan akaun pengguna lain; v. Pengguna perlu menukar kata laluan secara berkala; dan vi. Pengguna perlu mematuhi amalan terbaik keselamatan ICT dalam pemilihan dan penggunaan kata laluan.	Semua
2.0	***Unattended User Equipment***	
	Peralatan ICT yang diletakkan berjauhan dari pemilik/pengguna atau ditinggalkan bersendiriaan perlu mematuhi perkara-perkara berikut: i. Komputer yang idle dalam tempoh 15 minit akan di *lock screen*; ii. Peralatan ICT perlu *log off* setelah tugasan selesai; dan iii. Kawalan yang bersesuaian perlu dilaksanakan bagi peralatan tanpa pengawasan.	Semua
3.0	***Clear Desk* Dan *Clear Screen***	
	Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan- bahan yang sensitif terdedah sama ada di atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. i. Pengguna perlu *lock screen* apabila meninggalkan komputer pada bila-bila masa, jika tidak *screen* akan *dilock/hibernate* selepas 15 minit idle; ii. Fail atau dokumen terperingkat perlu disimpan di tempat yang berkunci apabila meninggalkan meja kerja; iii. Maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan; dan	Semua

	iv. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: i. Menggunakan *logout* apabila meninggalkan komputer; ii. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan iii. Memastikan dokumen diambil segera dari pencetak dan mesin fotostat.	
4.0	**Penggunaan Komputer**	
	Pengguna komputer Lembaga Zakat Negeri Kedah Darul Aman perlu mematuhi perkara berikut: i. Komputer Lembaga Zakat Negeri Kedah Darul Aman hendaklah digunakan untuk tugas rasmi sahaja; ii. Pengguna bertanggungjawab memastikan bahawa komputer perlu sentiasa mempunyai *antivirus* yang aktif dan terkini; iii. Komputer perlu didaftar pemiliknya dan pemilik berkenaan adalah bertanggungjawab menjaga keselamatan komputer tersebut sehingga komputer tersebut dilupuskan; iv. Ketua Pegawai/ Ketua Divisyen/ Pegawai Zakat Daerah adalah bertanggungjawab terhadap komputer gunasama, dan setiap pergerakkan komputer tersebut perlu direkodkan; v. Pegawai yang dibekalkan dengan *notebook*, komputer *tablet* dan *smart phone* dibenarkan untuk membawa pulang atau dibawa ke mana-mana dan pegawai adalah bertanggungjawab menjaga keselamatan aset berkenaan sepanjang masa; vi. Pentadbir Rangkaian Dan Keselamatan berhak untuk menyiasat kandungan mana-mana kategori komputer apabila menerima arahan daripada CDO atau ICTSO secara jarak jauh (*remote*) atau mendapatkan komputer tersebut dari pengguna; vii. Komputer milik Lembaga Zakat Negeri Kedah Darul Aman adalah dilarang digunakan oleh pihak ketiga tanpa kawalan dan pengawasan pegawai Lembaga Zakat Negeri Kedah Darul Aman; dan viii. Pegawai perlu melaporkan dengan segera sekiranya berlaku kehilangan komputer, *notebook*, komputer *tablet* atau *smart phone* kepada ICTSO dengan menyertakan salinan laporan Polis.	Semua

0504 Capaian Sistem Pengoperasian		
1.0	**Capaian Sistem Pengoperasian**	
	Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak benarkan. Keperluan capaian hendaklah sentiasa dipantau dan dikemas kini bagi memastikan hak capaian ini diberikan kepada pegawai yang dibenarkan sahaja. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian kepada sumber sistem komputer. Kemudahan ini juga perlu bagi: i. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; ii. Merekodkan capaian yang berjaya dan gagal; iii. Membekalkan kemudahan untuk pengesahan (bagi sistem kata laluan kunci digunakan, kualiti kata kunci perlu mendapat pengesahan); dan iv. Mengehadkan masa penggunaan rangkaian bagi pengguna. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: i. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Lembaga Zakat Negeri Kedah Darul Aman; ii. Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem; dan iii. Menyediakan tempoh penggunaan mengikut kesesuaian. Perkara-perkara yang perlu dipatuhi termasuk berikut: i. Mengawal capaian ke atas sistem operasi menggunakan prosedur *log on* yang terjamin ii. Mewujudkan satu pengenalan diri yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja dan satu teknik pengesahan yang bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna; iii. Mewujudkan fungsi pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah kukuh mengikut polisi kata laluan yang berkuatkuasa; iv. mengehadkan dan mengawal penggunaan program utiliti yang berkemampuan bagi satu tempoh yang ditetapkan; dan v. Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	Pengurus ICT

0505 Capaian Aplikasi Dan Maklumat		
	Bertujuan melindungi sistem maklumat dan aplikasi sedia ada daripada sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di Lembaga Zakat Negeri Kedah Darul Aman adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut perlu dipatuhi: i. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; ii. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini; iii. Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; iv. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; v. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja; vi. Maklumat tarikh log masuk terakhir hendaklah direkodkan; dan vii. *Session timeout* hendaklah dilaksanakan.	Pentadbir Sistem;
0506 Prosedur *Secure Log-on*		
	Capaian kepada sistem dan aplikasi hendaklah dikawal melalui prosedur *Log-on* mengikut keperluan. Pentadbir Sistem hendaklah mengenal pasti teknik pengesahan *log-on* yang sesuai seperti berikut: i. Tidak memaparkan sistem atau aplikasi selagi proses *log-on* tidak berjaya; ii. Paparkan suatu amaran bahawa sistem atau aplikasi hanya boleh diakses oleh pengguna yang sah; iii. Pengesahan *log-on*; iv. Perlindungan terhadap *Brute Force log-on*; v. Log “aktiviti *log on*” yang berjaya dan tidak berjaya;	Pentadbir Sistem;

	vi. Mengadakan amaran keselamatan jika ada potensi percubaan atau pencerobohan *log-on* berjaya dikesan; vii. Memaparkan tarikh dan masa *log-on* setelah selesai *log-on* yang berjaya; viii. Tidak memaparkan kata laluan; ix. Tidak menghantar kata laluan dalam "*clear-text*" melalui rangkaian; x. Menamatkan sesi yang tidak aktif selepas tempoh yang tertentu; dan xi. Menghadkan sesi sambungan sekatan untuk aplikasi yang berisiko tinggi	
0507 Capaian Jarak Jauh		
	Capaian jarak jauh yang dimaksudkan merangkumi: i. Capaian daripada sistem rangkaian dalaman; dan ii. Capaian daripada sistem rangkaian luaran bagi lokasi luar pejabat untuk tujuan *telecommuting.* Penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi (*encryption*); Lokasi bagi akses ke sistem ICT Lembaga Zakat Negeri Kedah Darul Aman hendaklah dipastikan selamat dan penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pentadbir Rangkaian dan Keselamatan. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.	Pentadbir Rangkaian dan Keselamatan; Semua
0508 Kawalan Capaian Rangkaian		
1.0	**Capaian Rangkaian**	
	Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: i. Mewujudkan segmen rangkaian yang bersesuaian bagi membezakan di antara rangkaian Lembaga Zakat Negeri Kedah Darul Aman dan rangkaian awam; ii. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dengan peralatan yang menepati kesesuaian penggunaannya; iii. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; iv. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dengan peralatan yang menepati kesesuaian penggunaannya;	Pentadbir Rangkaian dan Keselamatan

	v. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; vi. Capaian pengguna jarak jauh (*remote user*) perlulah dikawal dan dipantau; vii. Capaian fizikal dan logikal ke atas perkakasan rangkaian bagi tujuan mengubah konfigurasi perlulah dikawal; dan viii. Semua rangkaian yang dikongsi (*shared networks*), terutama yang keluar daripada rangkaian Lembaga Zakat Negeri Kedah Darul Aman, polisi perlu diwujudkan untuk mengawal capaian oleh pengguna.	
2.0	**Capaian Internet**	
	i. Penggunaan Internet di Lembaga Zakat Negeri Kedah Darul Aman hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian dan Keselamatan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code, virus* dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian Lembaga Zakat Negeri Kedah Darul Aman; ii. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. ICTSO berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya atas nasihat Pentadbir Rangkaian dan Keselamatan; iii. Polisi *Content Filtering* mestilah digunakan dan dipantau bagi mengawal akses Internet. Pengguna boleh memohon pengecualian mengikut fungsi kerja untuk pertimbangan; iv. Penggunaan proksi yang telah ditetapkan oleh Lembaga Zakat Negeri Kedah Darul Aman bagi mengawal akses Internet mengikut fungsi kerja dan mematuhi pekeliling semasa yang dikeluarkan; dan v. Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video streaming,downloading)* adalah perlu bagi menguruskan penggunaan *bandwidth* yang maksimum dan lebih berkesan,	Pentadbir Rangkaian dan Keselamatan

3.0	**Peralatan Dalam Rangkaian**	
	Bagi memastikan bahawa peralatan yang disambungkan kepada Rangkaian Lembaga Zakat Negeri Kedah Darul Aman tidak menjejaskan keselamatan maklumat dan capaian, maka perkara-perkara berikut hendaklah dipatuhi: i. Peralatan perlu disahkan bebas daripada virus dan perisian antivirus hendaklah dipasang dan masih aktif sepanjang masa; ii. Hanya peralatan yang telah berdaftar dibenarkan di sambungan (*join*) kepada rangkaian; iii. Setiap peralatan yang hendak disambung ke rangkaian perlu menggunakan *protocol* TCP/IP dan akan menggunakan IP address dan *domain name* yang ditetapkan oleh Pentadbir Rangkaian Dan Keselamatan; dan iv. Konfigurasi peralatan dalam rangkaian selepas daripada *switches* adalah menjadi tanggungjawab pengguna.	Pentadbir Rangkaian dan Keselamatan
4.0	**Capaian Ke Atas *Port* Untuk Tujuan Diagnostik**	
	Bagi memastikan bahawa *port* rangkaian tidak dicapai tanpa pengawasan, perkara berikut perlu dipatuhi oleh pengguna; i. *Port* yang tidak digunakan perlu *disable*; ii. Capaian fizikal dan logikal ke atas *port* untuk tujuan iii. Diagnostik perlu mendapat kebenaran pegawai yang diberikan kuasa; iv. Capaian oleh pegawai Lembaga Zakat Negeri Kedah Darul Aman hanya dibenarkan berasaskan kepada tugas dan skop kerja; dan v. Capaian oleh pihak ketiga perlu mendapat kelulusan dari ICTSO yang diberikan kuasa.	Pentadbir Rangkaian dan Keselamatan
5.0	**Pengasingan Dalam Rangkaian**	
	Rangkaian Lembaga Zakat Negeri Kedah Darul Aman perlu dibuat pengasingan menggunakan *Virtual Local Area Network*, *Zone* (Intranet, *Demilitarized Zone*, Internet) dan *Virtual Private Network* mengikut jenis perkhidmatan, pengguna, sensitiviti maklumat dan sistem.	Pentadbir Rangkaian dan Keselamatan
6.0	**Kawalan Penghalaan (*Routing*) Rangkaian**	
	Penghalaan perlu dikawal supaya ianya tidak disalah guna dengan memastikan perkara berikut: i. Konfigurasi *routing* perlu disemak dan disahkan sebelum dilaksanakan; ii. Semakan routing table perlu dibuat dari masa ke semasa; dan iii. *Routing* di dalam sistem rangkaian perlu dilaksanakan dengan betul dan terkawal.	Pentadbir Rangkaian dan Keselamatan

0509 Peralatan Mudah Alih		
	Perkara yang perlu dipatuhi adalah seperti berikut: i. Merekodkan aktiviti keluar masuk penggunaan peralatan mudah alih bagi mengesan pergerakan perkakasan tersebut daripada kehilangan atau kerosakan; ii. Peralatan mudah alih hendaklah disimpan atau dikunci di tempat yang selamat apabila tidak digunakan; dan iii. Memastikan peralatan mudah alih yang dibawa keluar dari pejabat perlu disimpan dan dijaga dengan baik bagi mengelakkan daripada kecurian.	Semua
0510 *Bring Your Own Device* (BYOD)		
	BYOD merupakan peralatan mudah alih persendirian seperti telefon pintar, *tablet* dan *laptop* yang digunakan oleh pengguna yang melaksanakan tugas rasmi melalui sambungan rangkaian Lembaga Zakat Negeri Kedah Darul Aman menggunakan kemudahan *Wi-Fi* Lembaga Zakat Negeri Kedah Darul Aman atau *data line* persendirian untuk akses kepada Internet tertakluk kepada DKICT Lembaga Zakat Negeri Kedah Darul Aman. Sebagai garis panduan, pengguna bertanggungjawab memastikan langkah-langkah keselamatan perlindungan berkaitan penggunaan BYOD seperti berikut: i. Mengelak risiko kebocoran maklumat rasmi; ii. Mengelakkan ancaman risiko keselamatan ICT; iii. Memastikan produktiviti pengguna tidak terjejas dalam menjalankan urusan rasmi Lembaga Zakat Negeri Kedah Darul Aman; dan iv. Meningkatkan integriti data. Perkara yang perlu dipatuhi adalah seperti berikut; i. Pengguna BYOD perlu memastikan keselamatan maklumat semasa menggunakan peralatan BYOD; ii. Pengguna BYOD adalah dilarang memasang perisian yang tidak dibenarkan oleh Lembaga Zakat Negeri Kedah Darul Aman; iii. Pengguna BYOD adalah dilarang memasang perisian yang mengganggu servis rangkaian Lembaga Zakat Negeri Kedah Darul Aman; iv. Mengaktifkan fungsi keselamatan katalaluan di setiap komputer riba /peranti; v. Perkakasan BYOD hendaklah dilindungi oleh perisian *antivirus* bagi mengelak penyebaran *virus/malware/trojan* dan lain-lain ke atas pengguna Lembaga Zakat Negeri Kedah Darul Aman yang lain;	Semua

	vi. Pengguna BYOD perlu memastikan peranti yang digunakan menggunakan teknologi penyulitan (*encryption*), tandatangan digital atau sebarang mekanisme bagi melindungi maklumat elektronik semasa ianya digunakan; vii. Pengguna BYOD adalah dilarang menyalin dan membawa keluar maklumat organisasi dengan menggunakan peranti mudah alih dan media storan seperti *thumb drive*, *external hard disk* dsb; viii. Pengguna BYOD perlu memadam dokumen elektronik dengan merincih secara elektronik/*'secure deletion'* selepas dokumen tidak lagi digunapakai; dan ix. Pengguna BYOD adalah dilarang meninggalkan komputer riba / peranti di ruang pejabat yang terbuka tanpa menguncikannya dengan kabel keselamatan. Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada penggunaan BYOD.	
0511 Penggunaan Media Sosial		
Objektif: Memahami dan mematuhi asas dalam penggunaan dan pemantauan media sosial bagi memastikan penggunaan media sosial dan pengaliran maklumat yang telus, berhemah dan memberi impak positif kepada Lembaga Zakat Negeri Kedah Darul Aman		
1.0	**Amalan Baik Pemaparan Media Sosial**	
	Media sosial merujuk kepada sejenis saluran komunikasi dalam talian yang membolehkan pengguna berinteraksi dengan mudah secara bebas, berkongsi dan membincangkan maklumat dengan menggunakan gabungan multimedia yang terdiri daripada teks, gambar, video dan audio. Pentadbir Portal Dan Media Sosial yang mengendalikan media sosial digalakkan untuk memasukkan kriteria dan kandungan yang relevan dengan Lembaga Zakat Negeri Kedah Darul Aman seperti berikut: i. Memaparkan perkataan "<jenis media sosial> Rasmi Lembaga Zakat Negeri Kedah Darul Aman". ii. Meletakkan jata Kerajaan Negeri Kedah Darul Aman dan logo rasmi Lembaga Zakat Negeri Kedah Darul Aman dengan jelas. iii. Menyediakan penyataan pengenalan media sosial. iv. Menyediakan kandungan dalam bidang kuasa rasmi. v. Memastikan bahasa yang digunakan mudah difahami oleh pengguna.	Pentadbir Portal Dan Media Sosial

2.0	**Panduan Umum Penggunaan Media Sosial**	
	Pentadbir Portal Dan Media Sosial perlu memastikan pelaksanaan panduan umum penggunaan media sosial seperti yang berikut: i. Mengenal pasti objektif utama penggunaan media sosial. ii. Memahami cara penggunaan setiap media sosial sebelum menggunakannya. iii. Mematuhi Kod Etika Perkhidmatan Awam dalam penggunaan media sosial dan mendapatkan khidmat nasihat sekiranya diperlukan. iv. Memastikan akaun media sosial rasmi adalah milik Lembaga Zakat Negeri Kedah Darul Aman dan bukan milik individu. v. Menggunakan platform media sosial yang mempunyai penggunaan yang tinggi di kalangan kumpulan sasaran atau orang awam. vi. Mengelakkan daripada mewujudkan akaun media sosial yang tidak mampu diselaras dan dipantau. vii. Mengelakkan komunikasi dengan pengguna yang bersikap agresif atau kasar.	Pentadbir Portal Dan Media Sosial
3.0	**Penggunaan Peribadi Media Sosial**	
	Penggunaan media sosial di kalangan pegawai Lembaga Zakat Negeri Kedah Darul Aman adalah tertakluk kepada peraturan-peraturan yang sedang berkuat kuasa bagi memastikan penggunaan media ini tidak menjejaskan imej peribadi dan imej Lembaga Zakat Negeri Kedah Darul Aman.	Semua
4.0	**Etika Penggunaan Media Sosial Oleh Pegawai**	
	Sepanjang menggunakan media sosial samada untuk tujuan rasmi atau peribadi, pegawai perlu memastikan etika penggunaan media sosial seperti yang berikut: i. Semua pegawai adalah terikat dengan terma dan syarat yang terkandung dalam Enakmen 23, Enakmen Lembaga Zakat Negeri Kedah Darul Aman 2015 dan arahan-arahan yang berkaitan yang menjadi teras kepada keperibadian atau tatakelakuan pegawai Lembaga Zakat Negeri Kedah Darul Aman. ii. Prinsip-prinsip penggunaan media sosial oleh pegawai sama ada dalam urusan rasmi ataupun peribadi adalah sama seperti yang terpakai bagi media-media yang lain. iii. Pegawai tidak digalakkan untuk menggunakan media sosial bagi tujuan peribadi semasa waktu pejabat samada menerusi peralatan komputer atau alat mudah alih yang dibekalkan oleh pejabat ataupun melalui peralatan peribadi.	Semua

	iv.	Pegawai boleh menggunakan media sosial secara peribadi di luar waktu pejabat tetapi perlu berhati-hati supaya tidak mendedahkan sebarang maklumat rasmi.	
	v.	Sebarang komen mengenai isu-isu yang melibatkan pentadbiran Lembaga Zakat Negeri Kedah Darul Aman atau yang berbentuk serangan peribadi hendaklah dielakkan.	
	vi.	Ketepatan dan sensitivity maklumat yang ingin disampaikan hendaklah disemak terlebih dahulu sebelum dihantar.	
	vii.	Pegawai perlu memastikan perkongsian dan penggunaan maklumat yang berkaitan dengan hak cipta dan harta intelek telah mendapat kebenaran daripada pihak yang berkenaan.	
	viii.	Sekiranya terdapat kesilapan pada sebarang maklumat yang telah dihebahkan, akui pada umum, buat pembetulan dan mohon maaf kepada pihak yang berkaitan secara terus dalam laman sosial yang terlibat.	

PERKARA 06: KAWALAN KRIPTOGRAFI

Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.		
1.0	**Enkripsi**	
	Pengguna hendaklah membuat penyulitan (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Pengguna
2.0	**Tandatangan Digital**	
	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Pentadbir Sistem; Pengguna
3.0	**Kawalan Penggunaan Kriptografi**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut; i. Membangun dan melaksanakan peraturan enkripsi untuk melindungi maklumat sensitif menggunakan kaedah kriptografi yang sesuai pada setiap masa; ii. Mengenal pasti tahap perlindungan penggunaan kriptografi dengan mengambil kira jenis, kekuatan dan kualiti algoritma yang diperlukan.	Pentadbir Sistem; Pengguna
4.0	**Penggunaan Infrastruktur Kunci Awam (PKI)**	
	Pengurusan ke atas Infrastruktur Kunci Awam (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Pentadbir Sistem

PERKARA 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif: Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan dan ancaman.		
0701 Keselamatan Kawasan		
	Perkara-perkara yang perlu dipatuhi (bergantung kepada hasil penilaian risiko) termasuk yang berikut: i. Sumber data atau *server*, peralatan komunikasi dan storan perlu ditempatkan di pusat data yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegah kebakaran; ii. Akses adalah terhad kepada warga Lembaga Zakat Negeri Kedah Darul Aman yang telah diberi kuasa sahaja dan dipantau pada setiap masa; iii. Pemantauan dibuat menggunakan Sistem CCTV atau peralatan-peralatan lain yang sesuai; iv. Peralatan keselamatan seperti CCTV dan pengimbas biometrik perlu diperiksa secara berjadual; v. Peralatan pemantauan suhu dan kebocoran penghawa dingin; vi. Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau bilau dan bencana; vii. Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; viii. Pihak luaran yang dibawa masuk mesti diawasi atau diiringi oleh pegawai bertanggungjawab di sepanjang tempoh di lokasi mengikut keperluan sewajarnya; ix. Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan dan laluan awam; x. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; xi. Memperkukuhkan dinding dan siling; dan xii. Mengehadkan jalan keluar masuk.	Semua
1.0	**Kawalan Masuk Fizikal**	
	Kawalan masuk fizikal perlu dikenal pasti dan dilaksanakan ke atas kawasan yang menempatkan infrastruktur rangkaian dan komunikasi, fasiliti pemprosesan atau tempat penyimpanan maklumat terperingkat. Keselamatan fizikal termasuk keselamatan perimeter seperti pembinaan dinding, pagar kawalan dan menghadkan jalan keluar masuk ke kawasan berkenaan. Akses ke kawasan pejabat dan kawasan larangan perlu dikawal bagi memastikan hanya warga Lembaga Zakat Negeri Kedah Darul Aman atau pihak yang diberi tanggungjawab sahaja dibenarkan masuk.	Semua

2.0	**Kawasan Larangan ICT**	
	Kawasan larangan ditakrifkan sebagai kawasan dimana terdapat aset ICT kritikal yang boleh menjejaskan operasi dan keselamatan maklumat secara keseluruhan jika tidak dikawal. Kawasan larangan ICT di Lembaga Zakat Negeri Kedah Darul Aman ialah Bilik *Main Distribution Frame* (MDF), Pusat Data (*Data Centre*) dan Bilik Stor Penyimpanan Peralatan ICT. Akses kepada kawasan larangan hendaklah dikawal dan kebenaran hanyalah kepada pegawai yang dibenarkan sahaja; dan pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan aktiviti mereka hendaklah dipantau atau diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	Semua
3.0	**Perlindungan Kawasan ICT Dari Ancaman Luar Dan Bencana Alam**	
	Kawalan dan perlindungan keselamatan ke atas kawasan yang mempunyai Aset ICT perlu mengambil kira ancaman dari perbuatan manusia ataupun bencana alam seperti kebakaran, banjir, gempa bumi dan lain-lain.	Semua
4.0	**Kawalan Kawasan Penghantaran Barangan Dan *Loading Area***	
	Kawasan penghantaran barangan dan *loading area* hendaklah dikawal dan perlu dipisahkan dari akses terus ke kawasan larangan.	Semua
0702 Keselamatan Aset ICT		
Objektif: Melindungi aset ICT dari kehilangan, kerosakan, kecurian aset serta gangguan kepada aset tersebut.		
1.0	**Peralatan dan Perkakasan ICT**	
	Aset ICT perlu dijaga dan dikawal dengan baik supaya ianya boleh digunakan sepanjang masa, perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; ii. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; iii. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; iv. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Rangkaian Dan Keselamatan;	Semua

	v.	Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;	
	vi.	Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini disamping melakukan imbasan ke atas media storan yang digunakan;	
	vii.	Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;	
	viii.	Peralatan sokongn ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;	
	ix.	Peralatan-peralatan kritikal perlu disokong oleh *Uninterrutable Power Supply* (UPS);	
	x.	Peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;	
	xi.	Peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;	
	xii.	Peralatan ICT yang hendak dibawa keluar dari premis Lembaga Zakat Negeri Kedah Darul Aman perlulah mendapat kelulusan oleh kakaitangan yang diberikan kuasa dan direkodkan bagi tujuan pemantauan;	
	xiii.	Peralatan ICT yang hilang hendaklah dilaporkan kepada Divisyen Pengurusan Aset, ICTSO dan Ketua Pegawai atau Ketua Divisyen atau Pegawai Zakat Daerah dengan segera serta laporan Polis Diraja Malaysia hendaklah disertakan;	
	xiv.	Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;	
	xv.	Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset Lembaga Zakat Negeri Kedah Darul Aman;	
	xvi.	Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pengurus ICT untuk dibaik pulih;	
	xvii.	Sebarang pelekat selain tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;	
	viii.	Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;	
	xix.	Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan;	
	xx.	Pengguna bertanggungjawab terhadap perkakasan, perisisan dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;	

	xxi. Pengguna hendaklah memastikan perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; xxii. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan xxiii. Memastikan suis ditutup bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
2.0	**Media Storan Digital**	
	Media storan digital merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti DVD-ROM, *thumb drive* dan media storan lain. Media storan digital perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: i. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; ii. Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja; iii. Media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; iv. Media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; v. Akses dan pergerakan media storan hendaklah direkodkan; vi. Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; vii. Mengadakan salinan atau pendua (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; viii. Media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan ix. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	Semua

3.0	**Media Tandatangan Digital**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; ii. Media ini tidak boleh dipindah milik atau dipinjamkan; dan iii. Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan selanjutnya.	Semua
4.0	**Media Perisian dan Aplikasi**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan Lembaga Zakat Negeri Kedah Darul Aman; ii. Sistem aplikasi dalaman tidak dibenarkan didemostrasi atau diagih kepada pihak lain kecuali dengan kebenaran ICTSO; iii. Lesen perisian daripada CD-ROM, disk atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan iv. *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua
5.0	**Utiliti Sokongan**	
	Utiliti sokongan perlu berada dalam keadaan terbaik dan mencukupi bagi menyokong sistem beroperasi. Utiliti sokongan ini termasuk bekalan elektrik, air, penghawa dingin, *generator*, alat komunikasi dan lain-lain.	Bahagian Pembangunan Dan Penyelenggaraan
6.0	**Penyelenggaraan Perkakasan**	
	Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti adalah terkawal. Perkara-perkara yang perlu dipatuhi termasuk yang tersenarai di bawah: i. Perkakasan perlu diselenggara mengikut spesifikasi yang telah ditetapkan oleh pengeluar; ii. Memastikan perkakasan hanya boleh diselenggara oleh pihak yang dibenarkan sahaja; iii. Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; iv. Menyemak dan menguji perkakasan sebelum dan selepas proses penyelenggaraan; v. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan	Pengurus ICT

	vi. Penyelenggaraan mestilah mendapat kebenaran daripada pegawai yang diberikan tanggungjawab menjaganya.	
7.0	**Aset ICT di Luar Premis**	
	Aset ICT seperti storan penyimpanan maklumat, komputer peribadi, komputer *tablet*, telefon mudah alih, *smart card*, dokumen atau lain-lain perkakasan yang berada di luar premis Lembaga Zakat Negeri Kedah Darul Aman perlu dilindungi dari risiko keselamatan seperti kecurian, kerosakan dan lain-lain Antara perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Aset yang hendak dibawa keluar dari premis perlu mendapat kebenaran; ii. Pegawai adalah bertanggungjawab sepenuhnya ke atas aset yang dibawa keluar; iii. Aset perlu dilindungi dan dikawal sepanjang masa; iv. Penyimpanan atau penempatan aset mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua
8.0	**Pembudayaan Penggunaan Teknologi Hijau**	
	Langkah-langkah amalan seperti berikut: i. Tidak menggunakan atau mengaktifkan *screen saver*. Ini disebabkan penggunaan *screen saver* akan menggunakan jumlah tenaga yang sama dengan penggunaan skrin yang aktif; ii. Memastikan monitor dalam keadaan *standby/hibernate* selepas 5 minit tidak aktif; iii. Memastikan kemudahan *power management* untuk komputer dan *notebook* diaktifkan; iv. Memastikan komputer ditutup dan suis dimatikan serta *plug* komputer dicabut dari soket elektrik apabila tidak digunakan untuk jangka masa panjang. Ini untuk mengelakkan arus elektrik masih aktif dalam sistem pendawaian menerusi *plug* komputer yang tidak dimatikan dan dicabut; v. Mengaktifkan kemudahan *duplex* dan *mode draf* pada pencetak sebagai *default*. Ini adalah untuk menjimatkan penggunaan kertas dan dakwat pencetak; vi. Mengaktifkan kemudahan *power-saving sleep mode* pada pencetak (jika ada); vii. Mengurangkan bilangan pencetak *stand-alone* dengan pewujudan pencetak rangkaian yang dapat dikongsi bersama; viii. Mengawal dokumen yang berkenaan sahaja untuk dicetak; ix. Menimbangkan kawalan mencetak di pencetak rangkaian berdasarkan kata nama pengguna; dan x. Memastikan supaya penggunaan kertas secara optimum.	Semua

9.0	**Pelupusan dan Guna Semula Perkakasan**	
	Pelupusan melibatkan aset ICT yang telah rosak, usang dan tidak boleh dibaiki yang dibekalkan oleh Lembaga Zakat Negeri Kedah Darul Aman dan di tempatkan di premis Lembaga Zakat Negeri Kedah Darul Aman. Aset ICT yang akan dilupuskan atau diguna semula, terutama yang mengandungi maklumat terperingkat atau perisian yang dilesenkan, perlu diuruskan dengan teratur dan selamat mengikut prosedur pelupusan semasa atau guna semula peralatan yang telah ditetapkan. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan Lembaga Zakat Negeri Kedah Darul Aman. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Kandungan perkakasan khususnya maklumat terperingkat hendaklah dihapuskan terlebih dahulu sebelum pelupusan atau diguna semula; ii. Pelupusan Aset ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; iii. Kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding*, *grinding*, *degauzing* atau pembakaran atau kaedah lain yang bersesuaian; iv. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat pendua; v. Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; vi. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; vii. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; viii. Pegawai Aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem pengurusan aset; ix. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan x. Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, hardisk, motherboard dan sebagainya;	Semua

	ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana divisyen atau pejabat zakat daerah; iii. Memindah keluar dari Lembaga Zakat Negeri Kedah Darul Aman mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab Divisyen Pengurusan Aset; dan v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
0703 Keselamatan Persekitaran		
Objektif: Melindungi aset ICT Lembaga Zakat Negeri Kedah Darul Aman dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.		
1.0	**Kawalan Persekitaran**	
	Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada ICTSO. Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: i. Merancang dan menyediakan pelan keseluruhan susun atur pusat data dengan teliti; ii. Ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; iii. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; iv. Bahan mudah terbakar hendaklah disimpan di luar kawasan bersesuaian dan berjauhan dari aset ICT; v. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; vi. Cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; vii. Peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya sekali (1) kali dalam setahun. Aktiviti dan keputusan ujian ini pelu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan viii. Akses kepada saluran *riser* dan rak *switches* hendaklah sentiasa dikunci;	Semua

2.0	**Bekalan Kuasa**	
	Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Peralatan ICT kritikal hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT. ii. Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*generator*) hendaklah digunakan bagi perkhidmatan kritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan; dan iii. Peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Divisyen Teknologi Maklumat; Divisyen Pembangunan Dan Penyelenggaraan;
3.0	**Kabel**	
	Kabel rangkaian hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut : i. Menggunakan kabel yang mengikuti spesifikasi yang telah ditetapkan; ii. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan iii. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan iv. Kabel perlu dilabelkan dengan jelas dan melalui trunking bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Divisyen Teknologi Maklumat
4.0	**Prosedur Kecemasan Persekitaran**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan Lembaga Zakat Negeri Kedah Darul Aman; dan ii. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Dan Kesihatan Pekerja Lembaga Zakat Negeri Kedah Darul Aman.	Semua
5.0	**Mekanisma Pelaporan Insiden Bukan ICT**	
	Semua pengguna yang terlibat haruslah melaporkan dan merekod sebarang kejadian atau kerosakan peralatan bukan ICT kepada pihak pentadbiran divisyen berkenaan.	Semua

6.0	**Mekanisma Kawalan Peralatan Sewaan/Ujicuba (*Proof of Concept*)**	
	Penerimaan: i. Peralatan yang diterima bebas daripada *virus, backdoor, worm* dan perkara-perkara yang boleh memberi ancaman kepada perkhidmatan ICT Lembaga Zakat Negeri Kedah Darul Aman. Penyelenggaraan: i. Capaian melalui rangkaian luar Lembaga Zakat Negeri Kedah Darul Aman adalah tidak dibenarkan; dan ii. Aktiviti penyelenggaraan adalah di bawah pengawasan Pentadbir Sistem dan Pentadbir Rangkaian Dan Keselamatan. Pemulangan: i. Maklumat yang tersimpan dalam storan perlu dihapuskan secara kekal (*secured delete*); dan ii. Memastikan semua maklumat Lembaga Zakat Negeri Kedah Darul Aman tidak tertinggal pada peralatan.	Pentadbir Sistem; Pentadbir Rangkaian Dan Keselamatan
0704 Keselamatan Dokumen		
Objektif: Melindungi maklumat Lembaga Zakat Negeri Kedah Darul Aman dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.		
1.0	**Dokumen**	
	Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: i. Dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terhad, Sulit, Rahsia atau Rahsia Besar; ii. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; iii. Kehilangan dan kerosakan ke atas jenis dokumen perlu dimaklumkan mengikut Prosedur Arahan Keselamatan; iv. Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa sepertimana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Arkib Negara Malaysia; dan v. Menggunakan penyulitan (*encryption*) ke atas dokumen rahsia rasmi yang disediakan, disimpan dan dihantar secara elektronik.	Semua

PERKARA 08: KESELAMATAN OPERASI

Objektif: Memastikan pengurusan operasi dan kemudahan pemprosesan maklumat berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.		
0801 Pengendalian Prosedur Operasi ICT		
	Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: i. Prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal; ii. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap; dan iii. Prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan dan diberikan nombor versi pindaan dan diluluskan oleh ICTSO.	Semua
0802 Kawalan Perubahan		
	Perubahan yang melibatkan perkakasan rangkaian dan komunikasi, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah dikemukakan oleh Pemilik Sistem atau Pentadbir Sistem ICT dan mendapat kebenaran daripada pegawai yang diberi kuasa; dan Sebarang perubahan komponen sistem ICT hendaklah mematuhi keperluan yang ditetapkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: i. Pengubahsuaian yang melibatkan perkakasan rangkaian dan komunikasi, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada ICTSO dan pemilik sistem terlebih dahulu; ii. Aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan iii. Aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Semua

0803 Pengasingan Tugas dan Tanggungjawab		
	Tugas dan tanggungjawab setiap pegawai perlu ditetapkan dan jelas bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; ii. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan iii. Perkakasan yang digunakan bagi membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	ICTSO

0804 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga		
Objektif: Memastikan penyampaian perkhidmatan pihak ketiga mematuhi tahap keselamatan yang ditetapkan selaras dengan perjanjian perkhidmatan.		
1.0	**Perkhidmatan**	
	Pihak ketiga perlu mematuhi terma dan syarat-syarat berkaitan kawalan keselamatan yang telah ditetapkan dalam perjanjian perkhidmatan. Perkara-perkara yang mesti dipatuhi seperti berikut: i. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; ii. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan iii. Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Pentadbir Sistem
2.0	**Pemantauan Perkhidmatan Pihak Ketiga**	
	Perkhidmatan, laporan dan rekod pihak ketiga perlu dipantau, disemak dan diaudit.	Pentadbir Sistem

0805 Perancangan dan Penerimaan Sistem		
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.		
1.0	**Perancangan Kapasiti**	
	Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem; Pentadbir Rangkaian Dan Keselamatan
0807 Penerimaan Sistem		
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Semua sistem baru termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. ii. Sebarang penyerahan atau penerimaan sistem baru perlu mendapat pengesahan/kelulusan pemilik sistem dan perlu melalui proses UAT (*User Acceptance Test*) dan FAT (*Final Acceptance Test*); dan iii. Penyelenggaraan sistem tersebut adalah berdasarkan manual operasi dan prosedur yang ditetapkan. Semua sistem baharu (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. Kriteria ini hendaklah merangkumi perkara berikut: i. Memenuhi kehendak dan keperluan pengguna; ii. Menggunakan perisian pembangunan yang sah; iii. Memenuhi ciri-ciri keselamatan bagi mengelakkan risiko pencerobohan dan sebagainya; dan iv. Memenuhi keperluan-keperluan teknologi semasa dan akan datang (Contoh: mampu menggunakan pelbagai platform, IPv6 *ready*).	Pentadbir Sistem; Pengguna

0808 Perisian Berbahaya		
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti *virus, trojan* dan sebagainya.		
1.0	**Perlindungan dari Perisian Berbahaya**	
	Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT dari perisian berbahaya: i. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti *antivirus*, IDS dan IPS mengikut prosedur penggunaan yang betul dan selamat; ii. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa; iii. Mengimbas semua perisian atau sistem dengan *antivirus* sebelum menggunakannya; iv. Mengemas kini paten *antivirus* dengan yang terkini; v. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; vi. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; vii. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; viii. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan	Pentadbir Rangkaian Dan Keselamatan
0809 Perlindungan Dari *Mobile Code*		
	Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Pentadbir Sistem
0810 *Housekeeping*		
Objektif: Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.		
1.0	***Backup Dan Restore***	
	i. Menguji sistem backup dan restore sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; ii. *Backup* hendaklah dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan *backup* bergantung pada tahap kritikal maklumat; iii. Menyimpan sekurang-kurangnya tiga (3) generasi (*backup*); dan iv. Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	Pengurus ICT

0811 Pemantauan		
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.		
1.0	**Pengauditan Dan Forensik ICT**	
	ICTSO mestilah bertanggungjawab merekod dan menganalisa perkara-perkara berikut: i. Sebarang percubaan pencerobohan kepada sistem ICT Lembaga Zakat Negeri Kedah Darul Aman; ii. Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), spam, pemalsuan (*forgery*, *phishing*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); iii. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; iv. Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; v. Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; vi. Aktiviti instalasi dan penggunaan perisian yang membebankan *bandwidth* rangkaian; vii. Aktiviti penyalahgunaan akaun *email*; viii. Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Rangkaian dan Keselamatan; dan ix. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian.	ICTSO
2.0	**Jejak Audit**	
	Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: i. Rekod setiap aktiviti transaksi; ii. Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; iii. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan iv. Maklumat akitiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.	Pentadbir Sistem

	Pentadbir Sistem yang berkaitan hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
3.0	**Sistem Log**	
	Fungsi-fungsi sistem log adalah seperti berikut: i. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; ii. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan iii. Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	Pentadbir Sistem
4.0	**Pemantauan Log**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; ii. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; iii. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; iv. Aktiviti pentadbiran dan operator sistem perlu direkodkan; v. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisa dan diambil tindakan sewajarnya; dan vi. Masa yang berkaitan dengan sistem pemprosesan maklumat dalam Lembaga Zakat Negeri Kedah Darul Aman atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.	Pentadbir Sistem
5.0	**Penyeragaman Waktu**	
	Sistem ICT Lembaga Zakat Negeri Kedah Darul Aman perlu mempunyai waktu yang seragam dengan *Network Time Protocol* (NTP) dikeluarkan oleh *Standard and Industrial Research Institute of Malaysia* (SIRIM).	Pentadbir Sistem

0812 Kawalan Teknikal Keterdedahan (*Vulnerability*)		
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.		
1.0	**Kawalan dari Ancaman Teknikal**	
	Maklumat mengenai ancaman teknikal sistem maklumat yang digunakan perlu diperolehi. Pendedahan organisasi kepada ancaman teknikal perlu dinilai bagi mengenalpasti tahap risiko yang bakal dihadapi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; ii. Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan iii. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem
2.0	**Pematuhan Keperluan Audit**	
	Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua

PERKARA 09: PENGURUSAN KOMUNIKASI

Objektif: Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan.		
0901 Pengurusan Keselamatan Rangkaian		
1.0	**Kawalan Infrastruktur Rangkaian**	
	Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: i. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; ii. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; iii. Peralatan mestilah lulus proses *Factory Acceptance Check* (FAC) dan ujian piawaian yang ditetapkan oleh SIRIM atau agensi piawaian antarabangsa semasa dikeluarkan serta lulus *Final Acceptance Test* setelah pemasangan dan konfigurasi; iv. *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Rangkaian Dan Keselamatan; v. Trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan Lembaga Zakat Negeri Kedah Darul Aman; vi. Perisian *sniffer* atau *network analyzer* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; vii. Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat Lembaga Zakat Negeri Kedah Darul Aman; viii. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; ix. Sebarang penyambungan rangkaian yang bukan di bawah kawalan Lembaga Zakat Negeri Kedah Darul Aman adalah tidak dibenarkan; x. Peralatan yang hendak disambung kepada rangkaian perlu bebas daripada *virus* dan mempunyai *antivirus* yang sah; xi. Capaian kepada rangkaian perlu dilaksanakan mengikut kategori yang telah ditetapkan iaitu intranet, internet dan *Demilitarized Zone*; xii. Sistem yang terdapat di dalam rangkaian intranet tidak dibenarkan dicapai dari internet kecuali menggunakan *Virtual Private Network* (VPN) dan dikawal oleh Divisyen Teknologi Maklumat;	ICTSO; Pentadbir Rangkaian Dan Keselamatan.

	i. Pihak ketiga adalah tidak dibenarkan untuk mencapai rangkaian intranet kecuali untuk kerja-kerja pembangunan atau penyelenggaraan sistem dengan kebenaran pemilik sistem; dan ii. Capaian kepada *Wi-Fi* hendaklah dikawal mengikut kategori pengguna.	
2.0	**Keselamatan Perkhidmatan Rangkaian**	
	Pengurusan bagi semua perkhidmatan rangkaian yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenalpasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian.	Pentadbir Rangkaian Dan Keselamatan
3.0	**Pengasingan Rangkaian**	
	Pengasingan rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian Lembaga Zakat Negeri Kedah Darul Aman.	Pentadbir Rangkaian Dan Keselamatan
0902 Pengendalian Media		
Objektif: Melindungi media mudah alih dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan perkhidmatan.		
1.0	**Penghantaran dan Pemindahan**	
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu dan perlu mematuhi prosedur yang ditetapkan.	Semua
2.0	**Prosedur Pengendalian Dan Pelupusan Media**	
	Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut: i. Melabelkan media mengikut tahap sensitiviti sesuatu maklumat; ii. Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; iii. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; iv. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; v. Menyimpan media di tempat yang selamat; dan vi. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	Semua

3.0	**Keselamatan Sistem Dokumentasi**	
	Sistem dokumentasi perlu disimpan dengan selamat dan dilindungi daripada capaian yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem didokumentasi adalah seperti berikut: i. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; ii. Menyedia dan memantapkan keselamatan sistem dokumentasi; dan iii. Mengawal dan merekodkan aktiviti capaian dokumentasi sedia ada.	Semua
0903 Pengurusan Pertukaran Maklumat		
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara Lembaga Zakat Negeri Kedah Darul Aman dan agensi luar terjamin.		
1.0	**Pertukaran Maklumat**	
	Pertukaran maklumat mesti mendapat kelulusan daripada Ketua Pegawai Eksekutif atau CDO. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; ii. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara Lembaga Zakat Negeri Kedah Darul Aman dengan agensi luar; iii. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari Lembaga Zakat Negeri Kedah Darul Aman; dan iv. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya (*email encryption*).	Semua
2.0	**Pengurusan Mel Elektronik (*Email*)**	
	Penggunaan *email* hendaklah mematuhi kod etika, garis panduan dan peraturan yang ditetapkan oleh Lembaga Zakat Negeri Kedah Darul Aman. Di antara perkara yang perlu dipatuhi oleh pengguna e-mail Lembaga Zakat Negeri Kedah Darul Aman ialah: i. Akaun atau alamat mel elektronik yang diperuntukan oleh Lembaga Zakat Negeri Kedah Darul Aman boleh digunakan semasa membuat urusan rasmi; ii. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui *email*;	Semua

	iii. Pengguna perlu memastikan saiz *email* yang dihantar tidak melebihi saiz yang ditetapkan oleh penerima; iv. Pengguna tidak dibenarkan menghantar lampiran (*attachment*) melebihi had yang ditetapkan; v. penghantaran lampiran dalam format atau extension "*.exe, *.bat" dan "*.com" tidak dibenarkan; vi. Pengguna hendaklah menyemak dan menentukan tarikh dan masa sistem komputer adalah sentiasa tepat; vii. Pengguna perlu memastikan *email* dibaca dan diambil tindakan segera; viii. Pengguna perlu memastikan *mailbox* mempunyai ruangan storan yang cukup terutama untuk transaksi di hujung minggu atau cuti; dan ix. Pengguna bertanggungjawab mengemaskini *mailbox* masing- masing.	
3.0	**Pengendalian Portal Rasmi**	
	Perkara-perkara yang perlu dipatuhi oleh Pentabir Portal Dan Media Sosial dalam pengendalian perkhidmatan Portal adalah seperti berikut: i. Notis hakcipta perlu diletakkan pada semua laman web rasmi seperti berikut: "Hakcipta Portal Rasmi Lembaga Zakat Negeri Kedah Darul Aman dan kandungannya yang termasuk maklumat, teks, imej, grafik, fail suara, fail video dan susunannya serta bahan-bahannya ialah kepunyaan Lembaga Zakat Negeri Kedah Darul Aman kecuali dinyatakan sebaliknya. Tiada mana-mana bahagian portal ini boleh diubah, disalin, diedar, dihantar semula, disiarkan, dipamerkan, diterbitkan, dilesenkan, dipindah, dijual atau diuruskan bagi tujuan komersial dalam apa bentuk sekalipun tanpa mendapat kebenaran secara bertulis yang jelas terlebih dahulu daripada Lembaga Zakat Negeri Kedah Darul Aman. Produk-produk lain, logo dan syarikat atau organisasi yang tercatat di dalam portal ini adalah kepunyaan syarikat atau organisasi tersebut." ii. Kenyataan Penafian (*Disclaimer*) perlu diletakkan pada semua laman web rasmi seperti: "Lembaga Zakat Negeri Kedah Daru Aman adalah tidak bertanggungjawab bagi apa-apa kehilangan atau kerugian yang disebabkan oleh penggunaan mana-mana maklumat yang diperolehi dari portal ini serta tidak boleh ditafsirkan sebagai ejen kepada, ataupun syarikat yang disyorkan oleh Lembaga Zakat Negeri Kedah Darul Aman." iii. Dasar Privasi dan Keselamatan perlu diletakkan pada semua laman web rasmi seperti: "Halaman ini menerangkan dasar privasi yang merangkumi penggunaan dan perlindungan maklumat yang dikemukakan oleh pengunjung. Sekiranya anda membuat transaksi atau menghantar e-mel mengandungi maklumat peribadi, maklumat ini mungkin akan dikongsi bersama dengan agensi awam lain untuk membantu penyediaan perkhidmatan yang lebih berkesan dan efektif. Contohnya seperti di dalam menyelesaikan aduan yang memerlukan maklumbalas dari agensi-agensi lain."	Pentabir Portal Dan Media Sosial

4.0	***Business Information System***	
	Maklumat yang terlibat dalam perkongsian data di antara sistem aplikasi perlu dilindungi.	Semua
0904 Perkhidmatan E-Dagang (*Electronic Commerce Services*)		
Objektif: Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.		
1.0	**E-Dagang**	
	Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan. Perkhidmatan E-dagang melalui kemudahan Internet adalah dibenarkan dengan kawalan bagi menjamin keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; ii. Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan iii. Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Semua
2.0	**Transaksi Atas Talian**	
	Maklumat yang terlibat dalam transaksi atas talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian dan pendedahan yang tidak dibenarkan.	Semua
3.0	**Maklumat Capaian Umum**	
	Maklumat yang dipaparkan perlu mempunyai tahap integriti yang tinggi dan dilindungi dari pindaan yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti yang berikut: i. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; ii. Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan	Semua

	iii. Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	
0905 Perkhidmatan Simpanan Data Atas Talian (*Cloud Storage*)		
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Setiap dokumen rasmi hanya dibenarkan disimpan di Perkhidmatan *Cloud Storage* yang disediakan. ii. Dokumen terperingkat yang disimpan di *public cloud storage* hendaklah menggunakan kaedah *encryption* terlebih dahulu sebelum dimuat naik. iii. Setiap dokumen yang disimpan di atas talian perlu ditetapkan kata laluan untuk membuka dokumen. iv. Memuat naik data peribadi ke dalam perkhidmatan *cloud storage* rasmi adalah dilarang sama sekali.	Semua

PERKARA 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

1001 Keselamatan Dalam Membangunkan Sistem dan Aplikasi		
Objektif: Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.		
1.0	**Keperluan Keselamatan Sistem Maklumat**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketetapan maklumat; ii. Ujian keselamatan hendaklah dijalankan ke atas sistem dan *input* data untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem dan output untuk memastikan data yang telah diproses adalah tepat; iii. Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan iv. Sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan. v. Pihak ketiga adalah tertakluk kepada perjanjian *Non-Disclosure Agreement* (NDA) bagi penggunaan data sebenar (*operational data*) pada persekitaran pengujian atau *Proof of Concept* (POC).	Pentadbir Sistem; Pemilik Sistem, Pihak Ketiga.
2.0	**Prosedur Pengendalian Dan Pelupusan Media**	
	Spesifikasi reka bentuk perlu memasukkan keperluan keselamatan sistem maklumat. Sekiranya sesuatu *off-the-shelves* produk diperolehi, pembekal perlu dimaklumkan berkenaan keperluan keselamatan.	Pentadbir Sistem;
1002 Kebolehpercayaan Pemprosesan Dalam Aplikasi		
Objektif: Untuk mengelak kesalahan, kecacatan, kerugian, pengubahsuaian yang tidak dibenarkan, penyalahgunaan maklumat dalam aplikasi atau kehilangan kepercayaan terhadap sistem.		
1.0	**Pengesahan Data *Input***	
	Data yang dimasukkan ke dalam aplikasi perlu disahkan untuk memastikan data adalah tepat dan betul.	Pemilik Sistem

2.0	**Kawalan Bagi Pemprosesan Dalaman**	
	Satu prosedur pengujian perlu diwujudkan di dalam aplikasi bagi mengesan sebarang kerosakan maklumat yang terhasil dari kesilapan dan kecacatan pemprosesan ataupun kesalahan yang disengajakan. Aktiviti-aktiviti pengujian didokumenkan dan hasil keputusan perlu disimpan dengan selamat.	Pentadbir Sistem
3.0	**Integriti Maklumat**	
	Satu penilaian terhadap risiko keselamatan perlu dijalankan untuk menentukan keperluan integriti maklumat dan bagi mengenal pasti kaedah yang paling bersesuaian untuk dilaksanakan.	Pemilik Sistem; Pentadbir Sistem
4.0	**Pengesahan Data *Output***	
	Data yang dikeluarkan daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem
1003 Keselamatan Fail Sistem		
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.		
1.0	**Kawalan Perisian (*Operational Software*)**	
	Kawalan perubahan kepada perisian perlu dilaksanakan bagi mengurangkan risiko kerosakan pada perisian. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: i. Proses pengemaskinian perisian hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang diberi tanggungjawab dan mengikut prosedur yang telah ditetapkan; ii. Kod atau atur cara sistem yang telah dikemas kini hanya boleh digunakan selepas diuji dan diluluskan untuk digunakan; iii. Mengaktifkan audit log bagi merekodkan aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; iv. Mengawal capaian ke atas kod sumber bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian;dan v. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal vi. Sistem konfigurasi perlu didokumenkan.	Pentadbir Sistem

2.0	**Kawalan Data Pengujian Sistem**	
	Data pengujian sistem perlu dipilih dengan teliti, dilindungi dan terkawal. Penggunaan data sebenar (*operational data*) yang melibatkan data personel atau data sensitif pada persekitaran pengujian adalah tertakluk kepada perjanjian *Non-Disclosure Agreement* (NDA).	Pemilik Sistem
3.0	**Kawalan Capaian kepada Kod Sumber (*Source Code*)**	
	Kawalan capaian kepada kod sumber perlu dilaksanakan bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian. Kod sumber (*source code*) bagi aplikasi dan perisian adalah menjadi hak milik Lembaga Zakat Negeri Kedah Darul Aman.	Pentadbir Sistem
1004 Keselamatan Dalam Proses Pembangunan dan Penyelenggaraan		
Objektif: Menjaga dan menjamin keselamatan sistem perisian aplikasi dan maklumat.		
1.0	**Kawalan Perubahan**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Perubahan dan pengubahsuaian ke atas sistem perisian aplikasi dan maklumat hendaklah dikawal, diuji, direkodkan dan disahkan melalui prosedur yang ditetapkan sebelum diguna pakai; ii. Pengujian terhadap perubahan dan pengubahsuaian ke atas sistem perisian aplikasi dan maklumat hendaklah dilaksanakan dalam persekitaran yang berasingan sama ada daripada produksi atau pembangunan;	Pentadbir Sistem; Pemilik Sistem

	iii. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; iv. Mengawal perubahan dan / atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; v. Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan vi. Menghalang sebarang peluang untuk membocorkan dan memanipulasikan maklumat Lembaga Zakat Negeri Kedah Darul Aman.	
2.0	**Keperluan Kajian Teknikal Terhadap Aplikasi Selepas Perubahan Sistem Pengoperasian**	
	Aplikasi perlu dikaji dan diuji apabila berlaku perubahan sistem pengoperasian bagi memastikan tiada sebarang kesan buruk yang merugikan kepada operasi dan keselamatan organisasi.	Pentadbir Sistem; Pemilik Sistem
1005 Pengurusan Kelemahan Teknikal		
Objektif: Mengurangkan Risiko Akibat dari Eksploitasi Kelemahan Teknikal.		
1.0	**Kawalan Kelemahan Teknikal**	
	Kelemahan teknikal terhadap sistem maklumat perlu dilapor dan dibuat penilaian dengan segera untuk tindakan pembetulan. Perkara yang perlu dipatuhi adalah seperti berikut: i. Memperoleh maklumat teknikal yang tepat pada masanya ke atas sistem maklumat yang digunakan; ii. Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan iii. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem; Pemilik Sistem

PERKARA 11: HUBUNGAN DENGAN PEMBEKAL/PIHAK KETIGA

1101 Pihak Ketiga		
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain)		
1.0	**Keperluan Keselamatan Kontrak dengan Pihak Ketiga**	
	Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara-perkara yang mesti dipatuhi seperti berikut: i. Membaca, memahami dan mematuhi DKICT Lembaga Zakat Negeri Kedah Darul Aman; ii. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; iii. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; iv. Akses kepada aset ICT Lembaga Zakat Negeri Kedah Darul Aman perlu berlandaskan kepada perjanjian kontrak; v. Mengenal pasti risiko ke atas keselamatan maklumat dan memastikan pelaksanaan kawalan yang sesuai ke atas maklumat tersebut; vi. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga, dan vii. Akses kepada aset ICT Lembaga Zakat Negeri Kedah Darul Aman perlu berlandaskan perjanjian kontrak. Perjanjian yang dimeterai perlu mematuhi perkara-perkara berikut: i. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga, perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. ii. *Non-Disclosure Agreement*; iii. Perakuan Akta Rahsia Rasmi 1972; dan viii. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT Lembaga Zakat Negeri Kedah Darul Aman	Pentadbir Sistem
1102 Pengurusan Penyampaian Perkhidmatan Pembekal, Pakar Runding dan Pihak-Pihak Lain Yang Terlibat		
Objektif: Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pembekal, pakar runding dan pihak-pihak lain yang terlibat.		

1.0	**Kawalan Keselamatan Maklumat Melalui Perjanjian Dengan Pembekal**	
	Lembaga Zakat Negeri Kedah Darul Aman hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal/pihak ketiga. Perkara yang perlu dipatuhi adalah: i. Memasukkan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat; ii. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa dan; iii. Pengurusan ke atas perubahan penyediaan perkhidmatan termasuk menyelenggara dan menambah baik polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua
2.0	**Pengurusan Perubahan Perkhidmatan Pembekal**	
	Perkara yang perlu diambil kira adalah: i. Perubahan dalam perjanjian dengan pembekal; ii. Perubahan yang dilakukan oleh Lembaga Zakat Negeri Kedah Darul Aman bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; iii. Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pegawai pembekal dan perubahan sub-kontraktor pembekal.	Semua

PERKARA 12: PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

1201 Mekanisme Pelaporan Insiden Keselamatan ICT		
Objektif: Memastikan insiden keselamatan ICT dan kelemahan dilapor dan disalur dengan cepat dan berkesan bagi meminimumkan proses pembaikan dan mengurangkan kesan insiden keselamatan ICT.		
1.0	**Mekanisme Pelaporan**	
	Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera: i. Maklumat didapati hilang, atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; ii. Sistem maklumat digunakan tanpa kebenaran iii. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; iv. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan v. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.	ICTSO; CERT&DRP; Semua
2.0	**Pelaporan Kelemahan Keselamatan**	
	Pengguna sistem dikehendaki melaporkan sebarang kelemahan sistem dengan segera bagi mengelak insiden keselamatan ICT.	Semua
1202 Pengurusan Maklumat Insiden Keselamatan ICT		
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.		
1.0	**Maklumat Insiden Keselamatan ICT**	
	Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada Lembaga Zakat Negeri Kedah Darul Aman. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:	CDO; ICTSO

	i. Menyimpan jejak audit, backup secara berkala dan melindungi integriti bahan bukti; ii. Menyalin bahan bukti dan merekodkan maklumat dan aktiviti penyalinan; iii. Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; iv. Menyediakan tindakan pemulihan segera; dan v. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	
2.0	**Pembelajaran Dari Insiden Kelemahan Maklumat**	
	Mewujudkan mekanisma bagi menentukan maklumat insiden keselamatan maklumat direkod untuk dianalisa dan dipantau.	Pengurus ICT
3.0	**Pengumpulan Bukti**	
	Bukti-bukti insiden keselamatan maklumat perlu dikumpul dan dikekalkan untuk tindakan perundangan (jika perlu).	Pengurus ICT

PERKARA 13: PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1301 Dasar Kesinambungan Perkhidmatan		
Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.		
1.0	**Pelan Kesinambungan Perkhidmatan**	
	Pelan Kesinambungan Perkhidmatan (*Business Continuity Plan* - BCP) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh pihak pengurusan Lembaga Zakat Negeri Kedah Darul Aman. Perkara-perkara berikut perlu diberi perhatian: i. Mengenal pasti tanggungjawab dan prosedur kecemasan atau pemulihan; ii. Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap *business process* bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; iii. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; iv. Mendokumentasikan proses dan prosedur yang telah dipersetujui; v. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; vi. Membuat *backup*; dan vii. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali. BCP mempunyai empat komponen utama iaitu: i. Pelan Pemulihan Bencana; ii. Pelan Tindakbalas Kecemasan; iii. Pelan Tindakbalas Insiden; dan iv. Pelan Komunikasi. BCP hendaklah mengandungi perkara-perkara berikut: i. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; ii. Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;	CDO; ICTSO; Pengurus ICT; Pemilik Sistem

	iii. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan iv. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh Salinan BCP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. BCP hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian pelan BCP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan yang terlibat mengetahui mengenai pelan tersebut, dan peranan mereka apabila pelan dilaksanakan. Salinan BCP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	
1302 *Redundancy*		
	Kemudahan pemprosesan maklumat perlu mempunyai redundancy yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan redundancy perlu diuji (*failover test*) keberkesanannya dari masa ke semasa.	Pengurus ICT

PERKARA 14: PEMATUHAN

1401 Pematuhan dan Keperluan Perundangan		
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak daripada pelanggaran kepada DKICT Lembaga Zakat Negeri Kedah Darul Aman		
1.0	**Pematuhan Dasar**	
	Setiap pengguna di Lembaga Zakat Negeri Kedah Darul Aman hendaklah membaca, memahami dan mematuhi DKICT Lembaga Zakat Negeri Kedah Darul Aman dan undang-undang atau peraturan-peraturan lain yang berkaitan. Semua aset ICT di Lembaga Zakat Negeri Kedah Darul Aman termasuk maklumat yang disimpan di dalamnya adalah hak milik Lembaga Zakat Zakat Negeri Kedah Darul Aman. Ketua Pegawai Eksekutif berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	Semua
2.0	**Pematuhan dengan Dasar, Piawaian Dan Keperluan Teknikal**	
	ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO
3.0	**Pematuhan Keperluan Audit**	
	Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua
4.0	**Keperluan Perundangan**	
	Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di Lembaga Zakat Negeri Kedah Darul Aman.	Semua
5.0	**Pelanggaran Dasar**	
	Pelanggaran dasar ini boleh diambil tindakan undang-undang dan tatatertib di bawah Akta Rahsia Rasmi 1972 dan Enakmen Lembaga Zakat Negeri Kedah Darul Aman 2015- Bahagian IV Tataterbib Dan Surcaj.	Semua

GLOSARI	
Active Directory (AD)	Teknologi Microsoft yang digunakan untuk mengurus komputer dan perkakasan lain dalam rangkaian.
Antivirus	Perisian yang mengimbas *virus* pada media storan, seperti cakera keras (*hard disk*) untuk sebarang kemungkinan adanya *virus*.
Aset Alih	Aset alih bermaksud aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
Aset ICT	Peralatan ICT termasuk komputer, media storan, *server*, *router*, *firewall*, rangkaian dan lain-lain.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Jalur lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi dalam jangka masa yang ditetapkan.
BYOD	*Bring Your Own Device*
CCTV	*Closed-circuit television* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
Clear Desk dan Clear Screen	Tidak meninggalkan dokumen data dan maklumat terperingkat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
CDO	*Chief Digital Officer* Ketua Pegawai Digital yang bertanggungjawabkan terhadap teknologi digital, infrastruktur data, tadbir urus data, analitis data, literasi digital, data terbuka dan teknologi pintar.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
DRC	*Disaster Recovery Centre* Pusat Pemulihan Bencana
DRP	*Disaster Recovey Plan* Pelan Pemulihan Bencana
Encryption	Enkripsi atau penyulitan. Proses enkripsi data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Email	Satu kaedah mengarang, menghantar, menyimpan dan menerima mesej melalui sistem komunikasi elektronik.

GLOSARI	
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information *theft/espionage*), penipuan*(hoaxes).*
ICT	*Information and Communication Technology*
ICTSO	ICT *Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi dan hanya boleh dicapai oleh pegawai dan mereka yang diberi kebenaran sahaja.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Contohnya: Network-based IPS yang akan memantau trafik rangkaian bagi sebarang kemungkinan serangan.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
ISMS	*Information Security Management System.*
LAN	Local Area Network Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	*Log-out computer* Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan *virus, trojan horse, worm, spyware* dan sebagainya.
Mailbox	Peti *mail* pengguna untuk menyimpan semua e-mel yang diterima dan dihantar pengguna.
Mobile Code	*Mobile code* merupakan perisian yang boleh dipindahkan antara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh Java Applet, ActiveX dan sebagainya pada pelayar internet.

GLOSARI	
NACSA	*National Cyber Security Agency* Agensi Keselamatan Siber Negara
NTP	*Network Time Protocol*
Off-the-shelves	Peralatan yang dihasilkan secara komersial, *ready made*, *standardized*, dan *regularly available equipment*, barangan, alat ganti, perisian, dan sebagainya.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi.
Rekod	Bahan dalam bentuk bertulis atau bentuk lain yang menyatakan fakta atau peristiwa atau selainnya merakamkan maklumat termasuklah kertas, dokumen, daftar, bahan bercetak, buku, peta, pelan, lukisan, gambar foto, mikrofilem, filem sinematograf, rakaman bunyi, rekod yang dihasilkan secara elektronik, tanpa mengira bentuk atau ciri-ciri fizikal dan apa- apa salinannya.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Server	Pelayan komputer
SIRIM	*Standard and Industrial Research Institute of Malaysia.*
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
VPN	*Virtual Private Network*
WAN	*Wide Area Network* Rangkaian yang merangkumi kawasan yang luas.
Worm	Sejenis *virus* yang boleh mereplikasi dan membiak dengan sendiri. Ia biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.

LAMPIRAN

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT (PEGAWAI)
LEMBAGA ZAKAT NEGERI KEDAH DARUL AMAN

NAMA (HURUF BESAR) : _____

NO. KAD PENGENALAN : _____

JAWATAN DAN GRED : _____

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT Lembaga Zakat Negeri Kedah Darul Aman*; dan

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

TANDATANGAN : .....

TARIKH : .....

.....

Pengesahan Ketua Pegawai Teknologi Maklumat

.....

TANDATANGAN & COP JAWATAN

TARIKH: .....

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT
(PELAJAR LATIHAN INDUSTRI)
LEMBAGA ZAKAT NEGERI KEDAH DARUL AMAN

NAMA (HURUF BESAR) : _____

NO. KAD PENGENALAN : _____

NAMA INSTITUT : _____

NO. MATRIK : _____

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT Lembaga Zakat Negeri Kedah Darul Aman*; dan

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

TANDATANGAN : .....

TARIKH : .....

.....

Pengesahan Ketua Pegawai Teknologi Maklumat

.....

TANDATANGAN & COP JAWATAN

TARIKH: .....

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT (AGENSI / PEMBEKAL)
LEMBAGA ZAKAT NEGERI KEDAH DARUL AMAN

NAMA (HURUF BESAR) : _____

NO. KAD PENGENALAN : _____

NAMA AGENSI / SYARIKAT : _____

NO. PENDAFTARAN SYARIKAT: _____

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT Lembaga Zakat Negeri Kedah Darul Aman*; dan

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

TANDATANGAN : .....

TARIKH : .....

.....

Pengesahan Ketua Pegawai Teknologi Maklumat

.....

TANDATANGAN & COP JAWATAN

TARIKH: .....

PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN PERKHIDMATAN LEMBAGA ZAKAT NEGERI KEDAH DARUL AMAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan- peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah Seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Saya faham bahawa segala rahsia rasmi dan suratan rasmi yang saya peroleh semasa berurusan dengan Lembaga Zakat Negeri Kedah Darul Aman dan tidak akan membocorkan, menyiarkan atau menyampaikan, sama ada secara lisan, bertulis atau dengan cara elektronik kepada sesiapa jua dalam apa-apa bentuk, sama ada dalam masa atau selepas berurusan dengan Lembaga Zakat Negeri Kedah Darul Aman dengan tidak terlebih dahulu mendapatkan kebenaran bertulis. Saya berjanji dan mengaku akan menandatangani satu akuan selanjutnya bagi maksud ini apabila urusan dengan perkhidmatan Lembaga Zakat Negeri Kedah Darul Aman telah selesai.

TANDATANGAN : .....

NAMA (HURUF BESAR) :.....

NO. KAD PENGENALAN :.....

JAWATAN :.....

NAMA AGENSI/SYARIKAT :.....

TARIKH :.....

PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN LEMBAGA ZAKAT NEGERI KEDAH DARUL AMAN APABILA TAMAT KONTRAK PERKHIDMATAN DENGAN LEMBAGA ZAKAT NEGERI KEDAH DARUL AMAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah Seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Dengan ini menjadi satu kesalahan di bawah Akta tersebut bagi saya menyampaikan dengan tiada kebenaran apa-apa rahsia rasmi atau suratan rasmi kepada mana-mana orang lain, sama ada atau tidak orang itu memegang jawatan dalam perkhidmatan Lembaga Zakat Negeri Kedah Darul Aman, sebelum dan selepas saya tamat kontrak perkhidmatan.

Saya mengaku bahawa tidak lagi ada dalam milik saya atau kawalan saya apa-apa perkataan kod rasmi, isyarat timbal, atau kata laluan rasmi yang rahsia atau apa-apa benda, suratan atau maklumat, anak kunci, lencana, alat meteri atau cap bagi atau yang dipunyai atau diguna, dibuat atau diadakan oleh Lembaga Zakat Negeri Kedah Darul Aman yang tidak dibenarkan berada dalam milikan atau kawalan saya.

TANDATANGAN : .....

NAMA (HURUF BESAR) :.....

NO. KAD PENGENALAN :.....

JAWATAN :.....

NAMA AGENSI/SYARIKAT :.....

TARIKH :.....

SENARAI PERUNDANGAN DAN PERATURAN

BIL	NAMA
1.	Akta Tandatangan Digital 1997;
2.	Akta Rahsia Rasmi 1972;
3.	Akta Jenayah Komputer 1997;
4.	Akta Hak Cipta (Pindaan) Tahun 1997;
5.	Akta Komunikasi dan Multimedia 1998;
6.	Akta 709 – Akta Perlindungan Data Peribadi 2010;
7.	Akta 658 – Akta Perdagangan Elektronik 2006;
8.	Akta 629 – Akta Arkib Negara 2003;
9.	Akta 606 – Akta Cakera Optik 2000;
10.	Akta 298 – Kawasan Larangan Tempat Larangan 1959;
11.	Akta 56 – Akta Keterangan 1950;
12.	Akta 825-Akta Anti Berita Tidak Benar (Pemansuhan) 2020
13..	Arahan Keselamatan;
14.	Arahan Teknologi Maklumat 2007;
15.	Garis Panduan IT Outsourcing Agensi-Agensi Sektor Awam 04/2006;
16.	Garis Panduan Pengurusan Rekod;
17.	Arahan 20 (Semakan Semula) – Dasar dan Mekanisme Pengurusan Bencana Negara;
18.	Arahan 24 – Dasar dan Mekanisme Pengurusan Krisis Siber Negara;
19.	Dasar Pengurusan Rekod dan Arkib Elektronik;
20.	Enakmen 23, Enakmen Lembaga Zakat Negeri Kedah Darul Aman 2015;
21.	Peraturan Kewangan Lembaga Zakat Negeri Kedah Darul Aman;

SENARAI PERUNDANGAN DAN PERATURAN

BIL	NAMA
22.	Tatacara Pengurusan Aset Alih;
23.	National Cyber Security Policy (NCSP);
24.	Garis Panduan Penerapan Etika Penggunaan Media Sosial Dalam Sektor Awam (MAMPU);
25.	Surat Arahan Ketua Pengarah MAMPU - Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC27001:2007 dalam Sektor Awam bertarikh 24 Nov 2010;
26.	Surat Pekeliling Am Bilangan 3 Tahun 2009 - Garis Panduan Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam;
27.	Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA);
28.	Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam.