DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (DKICT)

KEMENTERIAN PERTAHANAN

1 JANUARI 2017

VERSI 5.0

DASAR KESELAMATAN
TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)
KEMENTERIAN PERTAHANAN

1 JANUARI 2017

VERSI 5.0

SEJARAH DOKUMEN

VERSI	KELULUSAN	TARIKH KUAT KUASA
3.1	Mesyuarat Ketua – Ketua Jabatan dan Bahagian (KBB) Bil.1/2011	5 Januari 2011
4.0	Mesyuarat Jawatankuasa Pemandu ICT Kementerian Pertahanan Bil. 4/2013	30 Ogos 2013
5.0	Mesyuarat Jawatankuasa Pemandu ICT Kementerian Pertahanan Bil. 3/2017 bertarikh 4 April 2017	1 Januari 2017

ISI KANDUNGAN

04 PENGURUSAN ASET

05 KAWALAN CAPAIAN

06 KRIPTOGRAFI

07 KESELAMATAN FIZIKAL DAN PERSEKITARAN

08 KESELAMATAN OPERASI

09 KESELAMATAN KOMUNIKASI

10 PEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM

11 HUBUNGAN DENGAN PEMBEKAL

12 PENGURUSAN INSIDEN KESELAMATAN ICT

13 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

14 PEMATUHAN

PERUTUSAN

KETUA SETIAUSAHA

Assalamualaikum wbt. dan Salam Sejahtera,

Saya bersyukur kepada Allah SWT, kerana dokumen Dasar Keselamatan ICT (DKICT) MinDef v5.0 telah berjaya dihasilkan untuk rujukan seluruh warga MinDef termasuk awam dan tentera.

DKICT MinDef v5.0 ini adalah selari dengan perkembangan teknologi dan tuntutan semasa dalam memastikan aspek keselamatan ICT MinDef tidak berkompromi.

Tambahan lagi MinDef adalah merupakan sebuah agensi Critical National Information Infrastructure (CNII) yang bertanggungjawab terhadap keselamatan dan pertahanan negara.

DKICT MinDef v5.0 ini adalah merupakan peningkatan kepada DKICT MinDef v4.0 dengan mengambil kira keperluan piawaian keselamatan maklumat ISO/IEC 27001:2013 Information Security Management System (ISMS).

Bagi memastikan aspek keselamatan ICT MinDef sentiasa terkawal, saya memohon semua warga MinDef memahami, menghayati dan mematuhi kandungan dokumen ini serta menzahirkannya.

Semoga segala usaha kita ini akan mendapat keberkatan dan pertolongan daripadaNya jua.

Sekian, terima kasih.

DATO' SRI ABDUL RAHIM BIN MOHAMAD RADZI

PERUTUSAN

PANGLIMA ANGKATAN TENTERA

Assalamualaikum wbt. dan Salam Sejahtera,

Saya mengucapkan jutaan terima kasih kepada Bahagian Pengurusan Maklumat, Kementerian Pertahanan di mana telah berjaya menghasilkan Dasar Keselamatan ICT (DKICT) MinDef v5.0 yang akan digunakan sebagai rujukan, dasar dan polisi pengurusan keselamatan ICT bagi warga MinDef termasuk warga ATM.

Sejajar dengan arus pemodenan dan perkembangan teknologi ICT masa kini, ATM bergantung kepada penggunaan teknologi tersebut di dalam penugasan serta pengoperasian perkhidmatan. Oleh yang demikian, ATM telah melaksanakan pelbagai usaha ke arah memperkukuhkan system pengurusan keselamatan ICT. Ia merupakan *"strategic enabler"* yang berkeupayaan meningkatkan keberkesanan dan kecekapan keselamatan maklumat di dalam ATM. Justeru itu, pengurusan keselamatan ICT merupakan asas kepada keselamatan maklumat ATM dan negara.

Dengan penerbitan DKICT MinDef v5.0 ini, ia akan menjadi teras panduan keselamatan maklumat kepada semua warga MinDef dan ATM serta pihak yang berkaitan. Sungguhpun begitu, warga ATM haruslah sentiasa peka di dalam menjaga keselamatan maklumat agar tidak disebarkan atau diceroboh oleh pihak yang tidak berkepentingan.

Warga ATM bukan sahaja mampu berjuang di medan peperangan tetapi mesti mampu menjaga keselamatan maklumat dengan membudayakan *"best practice"* dalam pengurusan keselamatan ICT. Sehubungan dengan itu, saya menyeru agar semua warga ATM mematuhi dan menguatkuasakan DKICT MinDef v5.0 dengan membaca, memahami dan menjadikan keselamatan ICT sebagai satu lagi budaya kerja di dalam ATM.

Sekian, terima kasih.

"KESELAMATAN NEGARA, TANGGUNGJAWAB BERSAMA"

TAN SRI RAJA MOHAMED AFFANDI BIN RAJA MOHAMED NOOR
Jeneral
Panglima Angkatan Tentera

PERUTUSAN

KETUA PEGAWAI MAKLUMAT

Assalamualaikum wbt. dan Salam Sejahtera,

Pengurusan maklumat adalah merupakan salah satu komponen strategik dalam sesebuah organisasi. Bagi MinDef, komponen ini menjadi lebih kritikal supaya operasi bisnes tidak terganggu. Sebarang gangguan dalam operasi bisnes MinDef bukan sahaja menjejaskan tahap kesiapsiagaan bahkan boleh menggugat keselamatan negara.

Di dalam dunia digital hari ini, pengurusan maklumat adalah sentiasa terdedah kepada pelbagai tindakan oleh pihak yang berkepentingan untuk mengganggu, mengakses tanpa kebenaran dan menyebarkan maklumat rasmi kerajaan. Melalui teknologi, tindakan ini boleh dilakukan secara pantas dan meluas apabila sedikit sahaja ruang yang tersedia akibat dari kelemahan atau kecuaian. Oleh hal yang demikian kita perlu sentiasa berwaspada dalam menguruskan maklumat rasmi kerajaan supaya sentiasa dalam keadaan selamat.

Keselamatan adalah ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Bagi memastikan keselamatan sentiasa terpelihara, MinDef mengeluarkan dokumen DKICT v5.0 yang merupakan pengemaskinian kepada DKICT v4.0 sebagai panduan kepada semua warga MinDef dan pembekal dalam menjalankan tugas.

Justeru semua warga MinDef termasuk awam dan tentera adalah tertakluk kepada pematuhan dasar ini. Saya menyeru semua warga MinDef untuk bersama-sama memahami dan menghayati serta menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT MINDEF sebagai satu usaha murni dan ikrar kita untuk menjaga keselamatan maklumat kerajaan dan keselamatan negara umumnya.

Sekian, terima kasih.

DATO' MOHAMMAD FOAD BIN HAJI ABDULLAH

PENGENALAN

PENGENALAN

DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (DKICT)

KEMENTERIAN PERTAHANAN

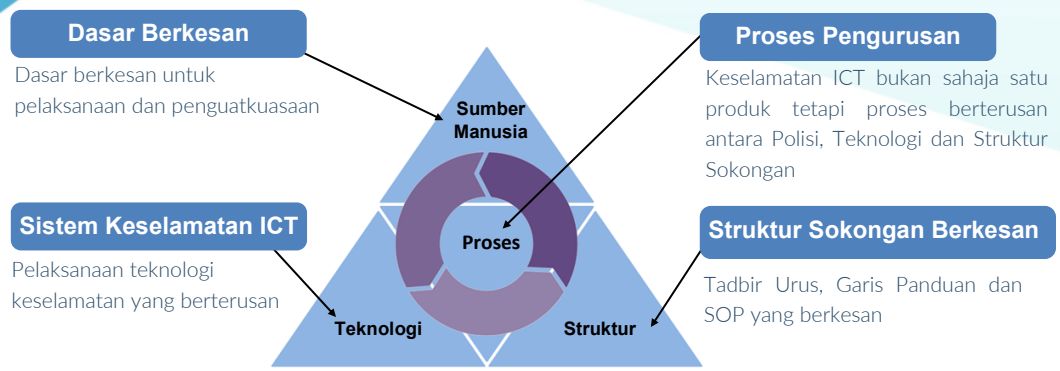
Perkembangan Teknologi Maklumat dan Komunikasi (ICT) yang pesat telah mengubah cara hidup dan budaya kerja organisasi. Keadaan yang semakin sofistikated ini turut merumitkan pengurusan keselamatan. Semua warga Kementerian Pertahanan (MinDef) perlu peka terhadap isu keselamatan ICT dalam melaksanakan peranan dan tanggungjawab yang ditetapkan. Justeru, kesedaran terhadap kepentingan keselamatan ICT memerlukan perhatian yang serius.

Fenomena ini menjadi semakin mendesak kerana MinDef adalah sebuah agensi *Critical National Information Infrastructure* (CNII) yang bertanggungjawab terhadap keselamatan dan pertahanan negara.

Kepelbagaian teknologi ICT telah membuka ruang kepada ancaman ke atas keselamatan aset ICT. Oleh hal yang demikian, mekanisme kawalan perlu dipertingkatkan untuk menjamin keselamatan dan ketersediaan maklumat.

Keselamatan ICT merupakan tanggungjawab warga MinDef untuk memastikan sistem ICT yang dikendalikan adalah selamat daripada sebarang penyalahgunaan dan ancaman pencerobohan. Satu dasar keselamatan diwujudkan bagi membantu pengurusan keselamatan ICT dilaksanakan dengan cekap dan berkesan.

Dasar Keselamatan ICT (DKICT) MinDef digambarkan seperti di **Rajah 1.**



Rajah 1 : Elemen dan Kepentingan DKICT MinDef

DKICT MinDef mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset ICT. Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT MinDef.

Rajah 2 : Bidang-bidang DKICT

OBJEKTIF

DKICT MinDef diwujudkan bagi menjamin kesinambungan bisnes MinDef dengan mencegah insiden atau meminimumkan kesan ke atas keselamatan aset ICT.

Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi MinDef. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi dengan selamat.

Objektif utama DKICT MinDef adalah:

a) Menghebahkan pendirian pihak pengurusan untuk mendukung pelaksanaan keselamatan ICT;

b) Menyediakan DKICT MinDef yang komprehensif, sesuai dengan perubahan masa dan diguna pakai oleh semua peringkat pengurusan dan pengguna;

c) Melindungi kepentingan aset dan pihak yang bergantung kepada sistem ICT daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan serta mencegah penyalahgunaan aset ICT;

d) Memastikan kelancaran operasi bisnes MinDef dengan mencegah serta meminimumkan kemusnahan dan kerosakan aset ICT; dan

e) Memberi kesedaran keselamatan ICT kepada warga MinDef dan pembekal.

PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Kawalan keselamatan adalah proses berterusan secara berkala yang mesti dilakukan untuk menjamin keselamatan.

Keselamatan ICT bermaksud keadaan di mana **segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan ICT beroperasi tanpa gangguan**.

Empat (4) komponen asas keselamatan ICT adalah:

a) Melindungi maklumat rasmi kerajaan dari capaian tidak sah;

b) Menjamin setiap maklumat adalah asli dan sempurna;

c) Memastikan ketersediaan maklumat apabila diperlukan; dan

d) Memastikan akses hanya diberi kepada pengguna yang sah dan penerimaan maklumat daripada sumber yang sah.

DKICT MinDef merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan dan ketersediaan maklumat. Ciri-ciri utama keselamatan maklumat adalah:

a) **Kerahsiaan** - Maklumat tidak boleh didedahkan atau dibiarkan akses tanpa kebenaran;

b) **Integriti** - Maklumat hendaklah asli, sempurna dan hanya boleh diubah dengan cara yang dibenarkan;

c) **Ketersediaan** - Maklumat hendaklah boleh diakses pada bila-bila masa;

d) **Tidak Boleh Disangkal** - Punca maklumat hendaklah daripada sumber yang sah dan tidak boleh disangkal; dan

e) **Kesahihan** - Maklumat hendaklah dijamin kesahihannya.

SKOP

Skop DKICT MinDef adalah:

a) Aset ICT MinDef;

b) Proses dan prosedur keselamatan ICT; dan

c) Tadbir urus keselamatan ICT.

DKICT MinDef merangkumi perlindungan ke atas semua bentuk maklumat kerajaan yang dikendalikan melalui penguatkuasaan sistem kawalan dan prosedur serta tadbir urus keselamatan aset ICT. Sebarang kebocoran maklumat atau kelemahan perlindungan dianggap sebagai pelanggaran langkah-langkah keselamatan.

PRINSIP-PRINSIP

Prinsip asas DKICT MinDef yang perlu dipatuhi adalah:

a) Akses atas dasar perlu mengetahui

Akses kepada sesuatu aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan akses tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan;

b) Hak akses minimum

Hak akses pengguna hanya diberi pada tahap paling minimum iaitu untuk tujuan rujukan sahaja. Keperluan akses selain daripada yang di atas seperti mewujudkan, menyimpan, mengemaskinikan, mengubah, membatalkan, menghapus, menyalin atau menyebar perlu mendapat kelulusan khas. Hak akses perlu disemak dari masa ke semasa berdasarkan kepada peranan, tanggungjawab serta bidang tugas pengguna;

c) Akauntabiliti

Semua pengguna adalah bertanggungjawab terhadap semua tindakannya ke atas aset ICT MinDef. Bagi menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong keupayaan untuk mengesan dan mengesahkan bahawa pengguna berkenaan boleh dipertanggungjawabkan atas tindakan mereka. Akauntabiliti pengguna adalah merangkumi perkara berikut:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

ii. Memeriksa maklumat dan menentukan keaslian dan kesempurnaan dari masa ke semasa;

iii. Menentukan ketersediaan maklumat;

iv. Menjaga kerahsiaan kata laluan;

v. Mematuhi standard, prosedur dan garis panduan keselamatan yang ditetapkan; dan

vi. Memberi perhatian kepada maklumat berdarjah terutama semasa pewujudan, pemprosesan, penyimpanan, penyelenggaraan, penyampaian, penyebaran, penukaran dan pemusnahan.

d) Pengasingan Fungsi

Pengasingan fungsi perlu dilakukan di antara pentadbir dan pengguna bagi mengelak capaian yang tidak dibenarkan. Pengasingan ini dapat mencegah berlakunya kesilapan, manipulasi serta kebocoran dan seterusnya mengekalkan integriti dan ketersediaan maklumat. Setiap fungsi sistem perlu diasingkan dengan jelas dan diberikan akses hanya kepada pengguna yang sah.

e) Pengauditan Keselamatan

Pengauditan keselamatan adalah tindakan untuk mengenal pasti risiko dan insiden keselamatan. Bagi tujuan tersebut, semua rekod log tindakan keselamatan dan jejak audit aset ICT seperti komputer, *server, firewall* dan rangkaian hendaklah dipelihara;

f) Pematuhan

DKICT MinDef hendaklah dibaca dan dipatuhi bagi mengelak sebarang bentuk pelanggaran yang boleh membawa ancaman kepada keselamatan aset ICT;

g) Pemulihan

Pemulihan sistem ICT adalah perlu untuk memastikan ketersediaan maklumat dan seterusnya meminimumkan gangguan atau kerugian. Pemulihan boleh dilakukan melalui aktiviti penduaan dan tindakan lain seperti yang dijelaskan dalam Pelan Kesinambungan Perkhidmatan dan Pelan Pemulihan Bencana; dan

h) Saling Bergantungan

Setiap prinsip adalah saling lengkap-melengkapi dan bergantung antara satu sama lain bagi menjamin keselamatan ICT yang maksimum.

BIDANG 1

PELAKSANAAN DASAR KESELAMATAN ICT

01 PELAKSANAAN DASAR KESELAMATAN ICT

Untuk menjelaskan hala tuju keselamatan ICT dan peraturan-peraturan bagi mengguna dan melindungi aset ICT selaras dengan keperluan undang-undang.

Bil	Perkara	Tanggungjawab
1.1	**Pelaksanaan Dasar Keselamatan ICT**	
	DKICT ini dilaksanakan oleh Ketua Setiausaha (KSU) dan Panglima Angkatan Tentera (PAT) dengan dibantu oleh Jawatankuasa Pemandu ICT (JPICT) MinDef yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan lain-lain pegawai yang dilantik.	**KSU/PAT**
1.2	**Penyebaran Dasar**	
	Dasar ini perlu disebarkan kepada semua warga MinDef dan pembekal yang berurusan dengan MinDef.	**CIO**
1.3	**Penyelenggaraan Dasar**	
	DKICT MinDef perlu disemak sekurang-kurangnya tiga (3) tahun sekali atau sekiranya ada keperluan. Prosedur penyelenggaraan DKICT MinDef adalah seperti berikut: a) Kenal pasti dan tentukan perubahan yang diperlukan; b) Mengemukakan cadangan perubahan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Pengurusan Tertinggi MinDef (MPT)/JPICT MinDef; dan c) Menyebarkan perubahan dasar yang telah dipersetujui kepada semua warga MinDef.	**ICTSO**

1.4	Pemakaian Dan Pengecualian Dasar	
	DKICT MinDef adalah terpakai kepada semua warga MinDef, pembekal dan pelawat yang berurusan dengan MinDef dan tiada pengecualian diberikan.	**Warga MinDef, Pembekal dan Pelawat**

BIDANG 2
ORGANISASI KESELAMATAN ICT

02 ORGANISASI KESELAMATAN ICT

Menerangkan peranan dan tanggungjawab semua pihak yang terlibat dengan lebih jelas dan teratur untuk mencapai objektif DKICT MinDef.

Bil	Perkara	Tanggungjawab
2.1	**Infrastruktur Organisasi Dalaman**	
2.1.1	**Ketua Setiausaha**	
	Peranan dan tanggungjawab Ketua Setiausaha (KSU) adalah: a) Memastikan pelaksanaan organisasi keselamatan ICT MinDef berfungsi dengan berkesan; b) Memastikan semua pengguna mematuhi DKICT MinDef; c) Memastikan semua keperluan keselamatan ICT (sumber kewangan, kakitangan dan perlindungan keselamatan) adalah mencukupi; d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT MinDef; dan e) Mempengerusikan Mesyuarat JPICT MinDef.	**KSU**
2.1.2	**Panglima Angkatan Tentera (PAT)**	
	Peranan dan tanggungjawab Panglima Angkatan Tentera (PAT) adalah: a) Memastikan pelaksanaan organisasi keselamatan ICT ATM berfungsi dengan berkesan; b) Memastikan semua pengguna mematuhi DKICT MinDef;	**PAT**

	c) Memastikan semua keperluan keselamatan ICT (sumber kewangan, kakitangan dan perlindungan keselamatan) adalah mencukupi; dan d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT MinDef.	
2.1.3	**Ketua Pegawai Maklumat**	
	Ketua Pegawai Maklumat (CIO) adalah pegawai yang dilantik oleh Ketua Jabatan mengikut Pekeliling Perkhidmatan Bilangan 5 Tahun 2007. Peranan dan tanggungjawab CIO adalah: a) Membantu KSU dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b) Menentukan keperluan keselamatan ICT; c) Menyelaras pembangunan dan pelaksanaan pelan tindakan dan program kesedaran mengenai keselamatan ICT; d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT; e) Mempengerusikan Mesyuarat JPICT MinDef dengan penurunan kuasa oleh KSU; dan f) Mempengerusikan Mesyuarat Jawatankuasa Keselamatan Maklumat MinDef.	**CIO**
2.1.4	**Pegawai Keselamatan ICT**	
	Pegawai Keselamatan ICT (ICTSO) adalah pegawai yang dilantik oleh Ketua Jabatan mengikut Pekeliling Perkhidmatan Bilangan 5 Tahun 2007. Peranan dan tanggungjawab ICTSO adalah:	**ICTSO**

	a) Menguatkuasakan dan memantau pematuhan DKICT MinDef; b) Mengurus keseluruhan program-program keselamatan ICT MinDef; c) Memberi penerangan dan pendedahan berkenaan DKICT MinDef kepada semua pengguna; d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT MinDef; e) Menjalankan tugas pengurusan risiko; f) Menjalankan audit, mengkaji, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti *malware* dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan (GCERT), Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia (MAMPU) dan memaklumkannya kepada CIO; i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan tindakan pemulihan dengan segera; j) Menyediakan dan melaksanakan program kesedaran mengenai keselamatan ICT; dan k) Mempengerusikan Mesyuarat Jawatankuasa Keselamatan Maklumat MinDef dengan penurunan kuasa oleh CIO.	
2.1.5	**Pengurus ICT**	

	Pengurus ICT adalah pegawai yang mengetuai bahagian ICT Jabatan dan perkhidmatan ATM. Peranan dan tanggungjawab Pengurus ICT adalah: a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MinDef; b) Menentukan kawalan akses semua pengguna terhadap aset ICT MinDef; c) Melaporkan sebarang insiden/penemuan ancaman keselamatan ICT kepada *Computer Emergency Response Team* (CERT) melalui Pegawai Keselamatan Maklumat Jabatan/Bahagian; dan d) Memastikan rekod, bahan bukti dan laporan terkini berkaitan keselamatan ICT MinDef disimpan bagi tujuan analisis dan siasatan.	**Pengurus ICT**
2.1.6	**Pegawai Keselamatan Maklumat Jabatan/Bahagian/Perkhidmatan ATM**	
	Pegawai Keselamatan Maklumat Jabatan/Bahagian/Perkhidmatan ATM adalah pegawai yang dilantik oleh KSU untuk bertanggungjawab bagi memastikan pengurusan dan pengendalian **Dokumen Rasmi MinDef** mematuhi semua arahan dan prosedur keselamatan yang ditetapkan. Peranan dan Tanggungjawab Pegawai Keselamatan Maklumat di Jabatan/Bahagian/Perkhidmatan ATM adalah seperti berikut: a) Bertanggungjawab ke atas semua aspek keselamatan dokumen dan maklumat rasmi Jabatan/Bahagian/Perkhidmatan ATM; b) Mewujud dan mempengerusikan Jawatankuasa Kecil Keselamatan Maklumat Jabatan/Bahagian/Perkhidmatan ATM;	**Pegawai Keselamatan Maklumat**

	c) Mengadakan pemeriksaan berjadual dan mengejut dari masa ke semasa ke atas aset ICT Jabatan/Bahagian; d) Mengambil tindakan yang bersesuaian ke atas sebarang penemuan mengenai keselamatan maklumat dengan segera; e) Memastikan penyimpanan rekod, bahan bukti dan laporan terkini mengenai ancaman dan insiden keselamatan dilaksanakan; f) Menyediakan laporan status dan penemuan mengenai keselamatan Dokumen Rasmi MinDef di Jabatan/Bahagian/ Perkhidmatan ATM setiap bulan kepada Jawatankuasa Keselamatan Maklumat MinDef; g) Melaksanakan kawalan keselamatan Dokumen rasmi MinDef berdasarkan kepada kerahsiaan, integriti dan ketersediaan maklumat; h) Memastikan semua aset ICT MinDef diberi kawalan akses dan perlindungan oleh pemilik aset yang berdaftar seperti yang ditetapkan; dan i) Mengemukakan cadangan untuk mengukuhkan langkah-langkah keselamatan dari masa ke semasa.	
2.1.7	**Pentadbir Sistem ICT**	
	Pegawai yang bertanggungjawab untuk menjalankan tugas-tugas pembangunan, penyelenggaraan dan pentadbiran sesuatu sistem ICT. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah: a) Memastikan kerahsiaan kata laluan dan konfigurasi aset ICT; b) Mengambil tindakan mengikut proses dan prosedur yang ditetapkan dengan segera apabila dimaklumkan mengenai pengguna yang berhenti, bersara, bertukar, bercuti panjang	**Pentadbir Sistem**

	atau berlaku perubahan dalam bidang tugas; c) Mengambil tindakan mengikut proses dan prosedur yang ditetapkan dengan segera apabila dimaklumkan mengenai pembekal yang berhenti atau tamat projek; d) Memastikan ketepatan dan kesempurnaan capaian seperti yang ditetapkan; e) Memastikan ketersediaan maklumat sepanjang masa; f) Memantau aktiviti capaian harian pengguna; g) Mengenal pasti aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan mengambil tindakan membatalkan atau memberhentikan serta merta capaian sistem seterusnya memaklumkan kepada Pengurus ICT untuk tindakan lanjut; h) Menganalisis dan menyimpan rekod jejak audit; dan i) Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	
2.1.8	**Pengguna**	
	Penjawat awam dan anggota tentera yang bekerja dan menggunakan rangkaian dan aset ICT di mana-mana organisasi di bawah Kementerian Pertahanan. Peranan dan tanggungjawab pengguna adalah: a) Mematuhi DKICT MinDef; b) Mengetahui dan memahami implikasi keselamatan ICT akibat dari tindakannya; c) Menjalani proses tapisan keselamatan seperti yang diarahkan; d) Mematuhi prinsip-prinsip DKICT MinDef dan menjaga	**Pengguna**

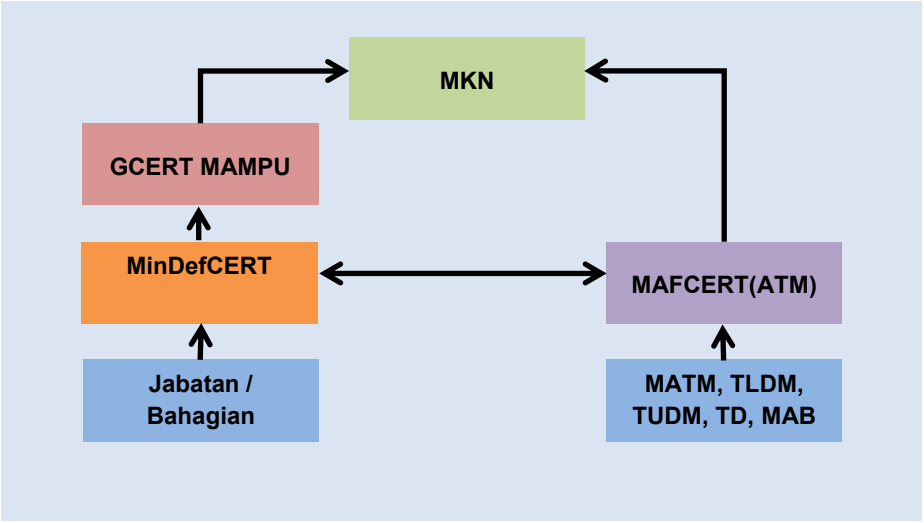
	kerahsiaan maklumat MinDef; e) Melaksanakan langkah-langkah perlindungan berikut: i. Tidak mendedahkan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia asli, tepat dan lengkap; iii. Menjaga kerahsiaan kata laluan; iv. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; dan v. Mengendalikan maklumat terperingkat mengikut proses dan prosedur yang ditetapkan. f) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada CERT melalui Pegawai Keselamatan Maklumat Jabatan/Bahagian/Perkhidmatan ATM dengan segera; g) Menghadiri program kesedaran mengenai keselamatan ICT; dan h) **Menandatangani "Surat Akuan Pematuhan" DKICT MinDef** (**LAMPIRAN A**).	
2.1.9	**Pembekal**	
	Individu atau kumpulan bukan warga MinDef yang menyediakan perkhidmatan ICT. a) Perkara yang perlu dipatuhi dalam berurusan dengan pembekal adalah seperti berikut: i. Mengenal pasti risiko keselamatan aset ICT serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;	**Pembekal**

	ii. Capaian kepada aset ICT MinDef perlu dinyatakan secara jelas dalam perjanjian perkhidmatan; dan iii. Memantau pelaksanaan tugas oleh pembekal supaya mematuhi perjanjian perkhidmatan berkaitan keselamatan ICT. b) Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian perkhidmatan: i. DKICT MinDef; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi (Pindaan) 1986; dan iv. Hak Harta Intelek. c) Pembekal hendaklah mematuhi perjanjian perkhidmatan yang ditetapkan.	
2.1.10	**Jawatankuasa Pemandu ICT MinDef (JPICT)**	
	Jawatankuasa Pemandu ICT MinDef (JPICT) adalah jawatankuasa yang bertanggungjawab untuk menilai dan meluluskan keperluan dan keselamatan ICT Jabatan/Bahagian/Perkhidmatan ATM. JPICT dipengerusikan oleh KSU/TKSU dengan keahlian terdiri daripada Ketua Jabatan/Bahagian/Perkhidmatan ATM yang dilantik dan diurus setia oleh BPM. **Bidang kuasa JPICT adalah:** a) Memperakukan, meluluskan dan menguatkuasakan dasar, hala tuju, garis panduan dan standard keselamatan ICT; b) Memantau tahap pematuhan keselamatan ICT; c) Memastikan DKICT MinDef selaras dengan dasar-dasar ICT semasa kerajaan;	**JPICT MinDef**

	d) Menerima dan membincangkan laporan mengenai insiden-insiden keselamatan ICT semasa; e) Membincang tindakan yang melibatkan pelanggaran DKICT MinDef; f) Meneliti dan meluluskan semua program dan aktiviti yang berkaitan dengan keselamatan ICT; g) Memastikan pengauditan keselamatan ICT MinDef dilaksanakan sekurang-kurangnya sekali setahun; dan h) Memastikan peruntukan kewangan yang mencukupi disediakan untuk pelaksanaan program dan aktiviti keselamatan.	
2.1.11	**Jawatankuasa Teknikal ICT MinDef (JTICT)**	
	Jawatankuasa Teknikal ICT MinDef (JTICT) adalah jawatankuasa yang bertanggungjawab untuk menilai dan menyokong aspek teknikal bagi keperluan dan keselamatan ICT Bahagian/Jabatan/ Perkhidmatan ATM. JTICT dipengerusikan oleh SUB BPM dengan keahlian terdiri daripada Pengurus ICT Jabatan/Bahagian/Perkhidmatan ATM dan wakil bahagian yang dikenal pasti dan diurus setia oleh BPM. **Bidang kuasa JTICT adalah:** a) Menilai aspek-aspek teknikal berhubung inisiatif dan projek keselamatan ICT; b) Memberi nasihat teknikal kepada JPICT MinDef; c) Menyediakan pelan tindakan untuk pembangunan dan peningkatan keselamatan sistem ICT; d) Menilai pilihan teknologi dan cadangan penyelesaian terhadap keperluan keselamatan sistem ICT; dan	**JTICT MinDef**

	e) Mengkaji semula DKICT dari masa ke semasa untuk dibentangkan kepada JPICT MinDef.	
2.1.12	**Organisasi *Ministry of Defense Computer Emergency Response Team* (MinDefCERT)**	
	Struktur organisasi MinDefCERT terdiri daripada Pengarah, Pengurus dan ahli-ahli yang dilantik. CIO adalah Pengarah MinDefCERT manakala ICTSO adalah Pengurus MinDefCERT. Ahli-ahli MinDefCERT terdiri daripada pegawai yang bertanggungjawab ke atas ICT jabatan/bahagian. Urus setia bagi MinDefCERT ialah BPM. **Bidang kuasa MinDefCERT adalah:** a) Menerima dan merekodkan aduan keselamatan ICT serta menilai tahap dan jenis insiden; b) Menjalankan siasatan ke atas insiden yang dilaporkan; c) Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan awal baik pulih; d) Menghubungi dan melaporkan insiden yang berlaku kepada *Government Computer Emergency Response Team,* Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (GCERT MAMPU) seperti di **Rajah 3;** e) Menasihatkan Jabatan/Bahagian supaya mengambil tindakan pemulihan dan pengukuhan; f) Memaklumkan sebarang ancaman dan insiden keselamatan ICT kepada Jabatan/Bahagian; dan g) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya	**MinDefCERT**

2.1.13	**Organisasi *Malaysian Armed Forces Computer Emergency Response Team* (MAFCERT)**	
	Struktur organisasi MAFCERT diketuai oleh Ketua Cyber Defence Operation Center (CDOC) dan dianggotai oleh semua wakil pengurus ICT perkhidmatan ATM (Markas ATM, Markas Angkatan Bersama, Markas Tentera Darat, Markas TUDM dan Markas TLDM). **Bidang kuasa MAFCERT adalah:** a) Menerima dan merekodkan aduan keselamatan ICT serta menilai tahap dan jenis insiden; b) Menjalankan siasatan ke atas insiden yang dilaporkan; c) Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minima; d) Menghubungi dan melaporkan insiden yang berlaku kepada Majlis Keselamatan Negara (MKN) seperti di **Rajah 3;** e) Menasihatkan Perkhidmatan ATM supaya mengambil tindakan pemulihan dan pengukuhan; f) Memaklumkan sebarang ancaman dan insiden keselamatan ICT kepada Perkhidmatan ATM; dan g) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	**MAFCERT**



Rajah 3 : Carta Pelaporan Insiden Keselamatan ICT MinDef

BIDANG 3
KESELAMATAN SUMBER MANUSIA

03 KESELAMATAN SUMBER MANUSIA

Memastikan semua sumber manusia yang menjadi pengguna aset ICT memahami tanggungjawab dan peranan, meningkatkan pengetahuan mengenai keselamatan aset ICT, mematuhi terma dan syarat perkhidmatan serta peraturan yang berkuat kuasa.

Bil	Perkara	Tanggungjawab
3.1	**Sebelum Perkhidmatan**	
	Perkara-perkara yang mesti dipatuhi adalah: a) Ketua Jabatan hendaklah menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pengguna/pembekal yang terlibat bagi menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b) Ketua Jabatan hendaklah menjalankan tapisan keselamatan ke atas pengguna dan pembekal mengikut keperluan perundangan, peraturan dan etika selaras dengan keperluan perkhidmatan, peringkat maklumat serta risiko yang dijangkakan; c) Semua pihak hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan; dan d) Ketua Jabatan perlu memastikan pengguna di bawah seliaannya menandatangani **Surat Akuan Pematuhan Dasar Keselamatan ICT MinDef** (**LAMPIRAN A**).	**Ketua Jabatan, Pengguna dan Pembekal**

3.2	**Semasa Perkhidmatan**	
	Perkara-perkara yang perlu dipatuhi termasuk: a) Pengguna dan pembekal yang berkepentingan hendaklah mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh MinDef; b) Ketua Jabatan hendaklah memastikan program kesedaran mengenai pengurusan keselamatan aset ICT diberi kepada pengguna secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka dan sekiranya perlu diberi kepada pembekal yang berkepentingan dari masa ke semasa; c) Ketua Jabatan hendaklah memastikan adanya proses tindakan disiplin/undang-undang ke atas pengguna/pembekal sekiranya berlaku pelanggaran perundangan dan peraturan MinDef; dan d) Semua pihak hendaklah memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan tujuan dan cara yang betul demi menjamin kepentingan keselamatan ICT.	**Ketua Jabatan, Pengguna dan Pembekal**
3.3	**Bertukar Atau Tamat Perkhidmatan**	
	Perkara-perkara yang perlu dipatuhi termasuk: a) Pengguna/pembekal hendaklah memastikan semua aset ICT dikembalikan kepada MinDef mengikut peraturan atau terma perkhidmatan yang ditetapkan; b) Pengguna/pembekal hendaklah membuat perakuan penyerahan aset ICT dan hak capaian ke atas maklumat dengan pengesahan penyelia; dan c) Pentadbir sistem hendaklah membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan	**Ketua Jabatan, Pentadbir Sistem, Pengguna dan Pembekal**

	pemprosesan maklumat yang diberikan kepada pengguna/ pembekal mengikut peraturan atau terma perkhidmatan yang ditetapkan oleh MinDef.	

BIDANG 4
PENGURUSAN ASET

04 PENGURUSAN ASET

Mengenal pasti dan melaksanakan tindakan bersesuaian bagi melindungi semua aset ICT MinDef.

Bil	Perkara	Tanggungjawab
4.1	**Tanggungjawab Ke Atas Aset ICT**	
4.1.1	Memastikan semua aset ICT kerajaan diberi kawalan dan perlindungan yang sewajarnya.	**Ketua Jabatan, Pentadbir Sistem dan Pengguna**
4.1.2	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Ketua Jabatan hendaklah mengenal pasti, mendokumenkan dan melaksanakan peraturan pengendalian aset; b) Ketua Jabatan hendaklah memastikan semua aset ICT dikenal pasti dan maklumat terkini aset direkod dalam sistem pengurusan aset; c) Ketua Jabatan hendaklah memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; d) Ketua Jabatan hendaklah memastikan semua aset ICT dikembalikan kepada MinDef mengikut peraturan atau terma perkhidmatan yang ditetapkan; dan e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	**Ketua Jabatan dan Pengguna**

4.2	**Pengelasan Maklumat**	
	Pengurusan maklumat yang melibatkan pewujudan, penyimpanan, pergerakan dan pelupusan hendaklah mengikut Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara serta proses dan prosedur yang berkuat kuasa.	**Ketua Jabatan, Pentadbir Sistem dan Pengguna**
4.2.1	**Klasifikasi dan Pelabelan Maklumat**	
4.2.1.1	Memastikan setiap maklumat diberi perlindungan yang bersesuaian berdasarkan tahap kerahsiaan.	
4.2.1.2	Maklumat hendaklah dikelas berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada kerajaan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: i. Rahsia Besar; ii. Rahsia; iii. Sulit; dan iv. Terhad.	**Ketua Jabatan, Pentadbir Sistem dan Pengguna**
4.2.2	**Pengendalian Maklumat**	
4.2.2.1	Pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan hendaklah mengikut standard, prosedur, garis panduan dan langkah keselamatan yang ditetapkan mengikut jenis-jenis pemprosesan berikut: a) Penyalinan; b) Muat naik (*upload*) dan muat turun (*download*); c) Penyimpanan dalam media storan;	**Pengguna**

	d) Penghantaran melalui pos, faks, e-mel dan media baharu seperti *Facebook*, *WhatsApp*, *Twitter*, *YouTube* dan *Instagram*; e) Penghantaran melalui percakapan termasuk melalui telefon bimbit, mel suara, mesin menjawab telefon dan *VoIP*; dan f) Pemusnahan.	
4.2.2.2	Langkah-langkah keselamatan yang perlu diambil adalah: a) Tidak mendedahkan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa, menyemak maklumat dan menentukan ia tepat dan lengkap dari masa ke semasa; c) Memastikan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan; e) Mematuhi standard, prosedur dan garis panduan keselamatan yang dikeluarkan dari masa ke semasa; f) Mematuhi tatacara pengendalian maklumat rasmi terperingkat terutama semasa pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan; dan g) Menjaga kerahsiaan tatacara pengurusan pengendalian maklumat rasmi keselamatan ICT dari diketahui umum.	**Pengguna**

JENIS-JENIS PEMPROSESAN	RAHSIA BESAR	RAHSIA	SULIT	TERHAD	TERBUKA
Penyalinan	KHAS	KHAS	KHAS	BIASA	BIASA
Penyimpanan	KHAS	KHAS	KHAS	BIASA	BIASA
Penyampaian	KHAS	KHAS	KHAS	BIASA	BIASA
Pemusnahan	KHAS	KHAS	KHAS	BIASA	BIASA

Rajah 4 : Matriks Penandaan Maklumat

Nota :

a) KHAS - Arahan Khas

b) BIASA - Terbuka iaitu boleh dilakukan

4.3	**Pengendalian Media**	
4.3.1	**Media Storan**	
4.3.1.1	Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat digital sama ada berbentuk kekal dan mudah alih. Contoh media storan yang digunakan adalah disket, pita magnetik, cakera keras, cakera optik dan kad memori. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Media storan hendaklah disimpan di ruang penyimpanan yang mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; c) Mewujudkan prosedur pengurusan media termasuk inventori, pergerakan, pelabelan dan *backup restore*; dan d) Penghantaran dan pelupusan media hendaklah dilaksanakan mengikut proses dan prosedur yang ditetapkan bagi menjamin keselamatan kandungan maklumat.	**Ketua Jabatan, Pengguna**

4.3.2	**Media Perisian**	
4.3.2.1	Media perisian yang digunakan untuk instalasi ke atas peralatan ICT perlu diberi penekanan kepada ciri-ciri keselamatan.	
4.3.2.2	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan MinDef; b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c) Lesen perisian (*registration code, serials number, CD-keys, hardcopy*) perlu disimpan secara berasingan dan selamat bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan d) *Source code* sesuatu sistem hendaklah disimpan mengikut proses dan prosedur yang ditetapkan.	**Pentadbir Sistem**
4.4	**Peralatan Mudah Alih**	
	Peralatan mudah alih seperti telefon pintar, *tablet* dan *laptop* yang digunakan untuk tujuan rasmi sama ada yang disediakan oleh jabatan atau milik persendirian hendaklah dipastikan mematuhi polisi dan prosedur yang ditetapkan	**Pengguna**
4.4.1	**Peralatan Yang Dibekalkan Oleh Jabatan**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Merekodkan pergerakan peralatan mudah alih bagi mengesan berlakunya kehilangan atau kerosakan; b) Peralatan mudah alih hendaklah disimpan atau dikunci di tempat yang selamat apabila tidak digunakan; dan c) Memastikan peralatan mudah alih yang dibawa keluar dari pejabat disimpan dan dijaga dengan baik bagi mengelakkan	**Pengguna**

	daripada kehilangan.	
4.4.2	**Peralatan Diperolehi Sendiri (BYOD)**	
	Rujuk kepada **LAMPIRAN C** berkaitan ***Bring Your Own Device* (BYOD).**	**Pengguna**

BIDANG 5
KAWALAN CAPAIAN

05 KAWALAN CAPAIAN

Mengehadkan akses ke atas maklumat dan kemudahan pemprosesan data.

Memastikan pengguna bertanggungjawab untuk melindungi maklumat yang digunakan.

Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem aplikasi.

Bil	Perkara	Tanggungjawab
5.1	**Keperluan Kawalan Capaian**	
5.1.1	**Polisi Kawalan Capaian**	
5.1.1.1	Polisi bagi mengawal capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan maklumat. Kawalan capaian hendaklah mengambil kira faktor *Identification, Authentication, Authorization, Accounting* dan *Non Repudiation* (IAAAN).	**CIO, ICTSO, Pengurus ICT, Pentadbir Sistem**
5.1.1.2	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Melaksanakan jejak audit; b) Mengawal penggunaan program utiliti yang boleh mengubah konfigurasi sistem; dan c) Mengurus kata laluan mengikut amalan terbaik serta prosedur yang ditetapkan oleh MinDef.	**Pentadbir Sistem**
5.1.1.3	Pengurusan Kata Laluan	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kata laluan hendaklah kukuh, dilindungi dan tidak boleh dikongsi atau didedahkan kepada sesiapa pun;	**Pentadbir Sistem, Pengguna**

	b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c) Kata laluan kukuh hendaklah sekurang-kurangnya lapan (8) aksara dengan gabungan huruf, nombor dan aksara khas; d) PC dan *notebook* hendaklah dilindungi dengan penggunaan *screen saver* dengan kata laluan untuk pengaktifan semula; e) Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan, pangkalan data atau media lain dan tidak boleh dikodkan di dalam program; f) Pertukaran kata laluan semasa *login* kali pertama atau selepas kata laluan diset semula perlu dikuat kuasa; g) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; h) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan i) Mengelakkan penggunaan semula kata laluan yang baharu digunakan.	
5.1.2	**Capaian Perkhidmatan Internet**	
5.1.2.1	**Kawalan Capaian Rangkaian**	
	Pengguna hendaklah diberikan akses hanya kepada perkhidmatan rangkaian yang telah ditetapkan. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Mewujudkan segmen rangkaian yang bersesuaian bagi membezakan had capaian pengguna dan keperluan sistem; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dengan peralatan yang menepati kesesuaian penggunaannya;	**Pentadbir Sistem**

	c) Memantau dan menguatkuasakan kawalan capaian pengguna ke atas perkhidmatan rangkaian ICT; d) Mewujudkan mekanisme pengesahan yang sesuai untuk mengawal capaian oleh pengguna luaran; dan e) Capaian fizikal dan logikal ke atas perkakasan rangkaian bagi tujuan mengubah konfigurasi perlulah dikawal.	
5.1.2.2	**Capaian Sistem Pengoperasian**	
	Memastikan bahawa capaian ke atas sistem pengoperasian dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mewujudkan satu pengenalan diri yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna yang berkenaan sahaja; b) Menamatkan sesi yang tidak aktif selepas tempoh masa yang ditetapkan; dan c) Mengehadkan tempoh hak capaian bagi meningkatkan keselamatan aplikasi yang berisiko tinggi.	**Pentadbir Sistem**
5.1.2.3	**Capaian Sistem Aplikasi**	
	Sistem aplikasi termasuk data dan maklumat perlu dilindungi dari sebarang bentuk capaian yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi adalah: a) Pengguna hanya boleh menggunakan sistem aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang ditetapkan; b) Setiap aktiviti capaian pengguna ke atas sistem aplikasi hendaklah direkodkan;	**Pentadbir Sistem**

	c) Capaian sistem aplikasi dari luar pejabat adalah terhad kepada perkhidmatan yang ditetapkan sahaja; dan d) Mengehadkan kawalan akses kepada kod sumber program.	
5.1.2.4	**Capaian Perkhidmatan Internet**	
	Capaian Internet perlu dikawal dan diurus bagi mengelakkan gangguan perkhidmatan ICT MinDef. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Penggunaan Internet di MinDef hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja; b) Kaedah *Content Filtering* hendaklah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan memantau tahap pematuhan; c) Pengurusan *bandwidth* hendaklah dilaksanakan untuk mengawal penggunaan *bandwidth* mengikut keperluan; d) Capaian perkhidmatan ICT strategik MinDef daripada luar pejabat hendaklah dipastikan selamat melalui penggunaan teknologi bersesuaian seperti VPN dan SSL; dan e) Pengguna yang diberi hak capaian adalah bertanggungjawab sepenuhnya ke atas penggunaan kemudahan yang diberikan. Rujuk **"Etika Penggunaan Internet dan E-mel Kementerian Pertahanan"** seperti di **LAMPIRAN B** dan Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".	**Pentadbir Sistem dan Pengguna**

5.2	**Pengurusan Kawalan Capaian Pengguna**	
	Pengurusan kawalan capaian pengguna ke atas sistem pengoperasian dan sistem aplikasi melalui rangkaian MinDef perlu dilaksanakan bagi menghalang capaian yang tidak sah.	**Pengurus ICT**
5.2.1	**Pendaftaran dan Pembatalan Akaun Pengguna**	
	a) Prosedur pendaftaran dan pembatalan hak capaian pengguna perlu diwujudkan dan didokumenkan; b) Setiap akaun pengguna adalah unik dan sebarang perubahan ke atas akaun pengguna mestilah mendapat kebenaran pihak pengurusan secara bertulis dan direkodkan; c) Pewujudan, pembatalan dan hak capaian akaun pengguna adalah tertakluk kepada peraturan jabatan. Tindakan pembatalan atau pengemaskinian akaun pengguna hendaklah diambil atas sebab seperti berikut: i. Pengguna tidak hadir bertugas tanpa kebenaran melebihi satu tempoh yang ditentukan oleh Ketua Jabatan; ii. Pengguna bercuti atau bertugas di luar pejabat melebihi satu tempoh yang ditentukan oleh Ketua Jabatan; iii. Pengguna bertukar jawatan, tanggungjawab atau bertukar bidang tugas; dan iv. Pengguna tidak lagi berkhidmat dengan MinDef sama ada bersara atau bertukar ke agensi lain.	**Pentadbir Sistem**
5.2.2	**Semakan Capaian Pengguna *(Provisioning)***	
	Semakan capaian pengguna hendaklah dilaksanakan untuk menilai semula capaian mengikut keperluan organisasi dari masa ke semasa.	**Pengurus ICT, Pentadbir Sistem**

5.2.3	**Pengurusan *Priviledge Access Rights***	
	Prosedur kawalan capaian perlu diwujudkan dan didokumenkan. Tahap capaian pengguna hendaklah sentiasa dipantau dan dikemaskinikan mengikut keperluan semasa.	**Pengurus ICT, Pentadbir Sistem**
5.2.4	**Pengurusan Pengesahan Pengguna**	
	Maklumat pengesahan pengguna hendaklah dirahsiakan dan diuruskan dengan berkesan.	**Pentadbir Sistem**
5.2.5	**Tanggungjawab Pengguna**	
	Setiap pengguna adalah bertanggungjawab ke atas: a) Akaun pengguna masing-masing selepas pengesahan penerimaan dibuat; dan b) Memelihara kesahihan dan tahap kerahsiaan maklumat yang dikendalikan.	**Pengguna**

BIDANG 6
KRIPTOGRAFI

06 KRIPTOGRAFI

Memastikan kerahsiaan, integriti dan kesahihan maklumat dilindungi melalui penggunaan kriptografi yang sesuai dan berkesan.

Bil	Perkara	Tanggungjawab
6.1	**Dasar Kriptografi**	
6.1.1	Peraturan bagi melindungi maklumat terperingkat menggunakan kaedah kriptografi yang sesuai dengan keperluan organisasi hendaklah diwujudkan dan dilaksanakan selaras dengan dasar dan peraturan yang berkuat kuasa.	**ICTSO**
6.1.2	Keperluan kawalan kriptografi mestilah dinyatakan dalam semua perolehan dan pembangunan ICT baharu yang melibatkan maklumat terperingkat. Kaedah, kod sumber dan produk kriptografi yang digunakan mestilah boleh diakses oleh Kerajaan bagi tujuan kawalan, penilaian dan penganalisaan keselamatan.	**Pengurus ICT**
6.2	**Pengurusan Kunci**	
6.2.1	Semua kunci kriptografi yang dihasilkan bagi melindungi maklumat terperingkat adalah milik Kerajaan.	**ICTSO, Pentadbir Sistem, Pengguna**
6.2.2	Kunci kriptografi mestilah dilindungi dengan menggunakan kaedah yang ditetapkan dan hendaklah dirahsiakan.	**Pentadbir Sistem, Pengguna**
6.2.3	Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut.	**Pentadbir Sistem, Pengguna**

6.3	**Tandatangan Digital**	
	Setiap urusan transaksi elektronik yang melibatkan maklumat terperingkat hendaklah menggunakan tandatangan digital bagi tujuan perlindungan kesahihan dan integriti. Kemudahan tandatangan digital yang digunakan hendaklah mematuhi dasar dan peraturan yang berkuat kuasa.	**Pentadbir Sistem, Pengguna**

BIDANG 7
KESELAMATAN FIZIKAL DAN PERSEKITARAN

07 KESELAMATAN FIZIKAL DAN PERSEKITARAN

Mencegah akses fizikal yang tidak dibenarkan dan boleh menjadi ancaman kehilangan, kerosakan, kecurian atau kompromi terhadap aset dan gangguan kepada pemprosesan maklumat MinDef.

Bil	Perkara	Tanggungjawab
7.1	**Keselamatan Persekitaran**	
7.1.1	**Perimeter Keselamatan Fizikal**	
	Perimeter keselamatan hendaklah ditakrifkan dan digunakan untuk melindungi **Kawasan Larangan** dan **Tempat Larangan** yang mengandungi maklumat sensitif atau kritikal dan juga kemudahan pemprosesan maklumat.	**Ketua Jabatan**
7.1.2	**Kawasan Larangan**	
	Kawasan Larangan ditakrifkan sebagai kawasan fizikal yang telah diwartakan sebagai kawasan larangan dan juga sebarang kawasan yang dihadkan kepada pegawai yang diberi kebenaran sahaja. Perkara–perkara yang perlu dipatuhi adalah seperti berikut: a) Kawalan keselamatan fizikal hendaklah dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. b) Prosedur kerja di kawasan larangan hendaklah diwujudkan dan dilaksanakan.	**Ketua Jabatan**
7.1.3	**Kawalan Kawasan Larangan**	
	Kawalan Kawasan Larangan adalah bertujuan untuk mengesan, mencegah dan menghalang cubaan untuk menceroboh ke kawasan	**Ketua Jabatan**

	yang menempatkan aset ICT MinDef. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mengenal pasti kawasan keselamatan fizikal dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset berasaskan penilaian risiko; b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan; c) Memasang alat penggera atau kamera (CCTV); d) Mempamerkan tanda kawasan larangan; e) Mengehadkan laluan keluar masuk; f) Mengadakan kaunter kawalan; g) Menggunakan sistem pas keselamatan; dan h) Melaksanakan perkhidmatan kawalan keselamatan terutama kawasan penghantaran dan pemunggahan.	
7.1.3.1	**Kawalan Masuk Dan Keluar Fizikal**	
	Kawalan masuk dan keluar fizikal adalah ditakrifkan sebagai kawalan ke atas warga MinDef dan pelawat yang masuk dan keluar premis. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap warga MinDef hendaklah memakai Pas Keselamatan sepanjang waktu bertugas; b) Semua Pas Keselamatan hendaklah diserahkan kembali apabila pegawai tamat perkhidmatan di MinDef;	**Warga MinDef, Pelawat**

	c) Setiap pelawat hendaklah mendapatkan Pas Pelawat di pintu masuk utama MinDef; d) Pas Pelawat ini hendaklah dikembalikan selepas tamat lawatan; dan e) Kehilangan pas mestilah dilaporkan dengan segera mengikut tatacara yang sedang berkuat kuasa di MinDef.	
7.1.4	**Kawalan Tempat Larangan**	
	Tempat Larangan ditakrifkan sebagai bangunan yang menempatkan aset ICT berisiko tinggi dan dihadkan kemasukan dengan kebenaran khas.	
7.1.4.1	Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a) Melindungi tempat larangan melalui sistem kawalan fizikal yang bersesuaian; b) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana; c) Menyediakan garis panduan untuk warga MinDef dan pelawat yang bekerja di dalam tempat larangan; d) Melengkapi semua ruang pejabat khususnya tempat yang mempunyai kemudahan ICT dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; e) Memasang peralatan perlindungan di tempat yang bersesuaian, mudah dikenali dan dikendalikan; f) Menyimpan bahan mudah terbakar di luar kawasan penyimpanan aset ICT;	**Ketua Jabatan**

	g) Memeriksa dan menguji semua peralatan perlindungan mengikut tatacara dan jadual yang ditetapkan. Aktiviti dan keputusan ujian ini perlu direkod untuk rujukan dan tindakan sekiranya perlu; h) Memastikan suhu premis mengikut spesifikasi yang ditetapkan; dan i) Peralatan ICT seperti *server*, peralatan keselamatan dan peralatan rangkaian yang kritikal perlu disokong oleh *Uninterruptible Power Supply* (UPS).	
7.2	**Keselamatan Peralatan ICT**	
7.2.1	Peralatan ICT hendaklah dijaga dan dikawal dengan baik bagi mengelak dari sebarang kehilangan, kerosakan, kecurian atau kompromi ke atas aset ICT dan gangguan ke atas sistem penyampaian agensi. Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalan berfungsi dengan baik; b) Pengguna bertanggungjawab sepenuhnya ke atas peralatan ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan, perubahan konfigurasi atau memindah kedudukan peralatan ICT yang dipasang tanpa kebenaran; c) Hanya perisian yang tulen, berdaftar dan dilindungi di bawah peraturan yang ditetapkan sahaja dibenarkan bagi kegunaan pengguna; d) Pengguna adalah bertanggungjawab atas kerosakan dan kehilangan peralatan ICT di bawah kawalan; e) Pengguna mesti memastikan peralatan ICT dilengkapi dengan	**Pentadbir Sistem, Pegawai Aset, Pengguna**

	perisian antivirus dan dikemaskinikan serta melakukan imbasan ke atas media storan yang digunakan; e) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; f) Semua peralatan sokongan ICT seperti peranti kad pintar hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; g) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada pegawai yang bertanggungjawab untuk tindakan lanjut; h) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset seperti yang ditetapkan mengikut proses dan prosedur yang berkuat kuasa; i) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; j) Peralatan ICT yang hendak dibawa keluar dari premis MinDef, perlulah mengikut proses dan prosedur yang berkuat kuasa; k) Penggunaan peralatan ICT hendaklah bagi urusan rasmi sahaja; l) Pengguna hendaklah memastikan semua peralatan ICT dimatikan suis bekalan kuasa apabila meninggalkan pejabat; dan m) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa.	
7.2.2	**Penyenggaraan Peralatan ICT**	
7.2.2.1	Peralatan ICT hendaklah diselenggarakan mengikut proses dan prosedur yang ditetapkan bagi memastikan kerahsiaan, integriti dan ketersediaan.	

7.2.2.2	Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a) Melaksanakan selenggaraan berdasarkan spesifikasi pengeluar; b) Memastikan peralatan ICT hanya diselenggarakan oleh pihak yang dibenarkan sahaja; c) Memeriksa dan menguji semua peralatan ICT sebelum dan selepas proses penyelenggaraan mengikut prosedur yang ditetapkan; dan d) Memaklumkan kepada pengguna sebelum melaksanakan penyelenggaraan.	**Pegawai Aset, Pentadbir Sistem dan Pengguna**
7.2.3	**Peminjaman Peralatan ICT Bagi Kegunaan Di Luar Pejabat**	
7.2.3.1	Peminjaman peralatan ICT bagi kegunaan di luar pejabat hendaklah mengikut proses dan prosedur yang berkuat kuasa bagi memastikan kerahsiaan, integriti dan ketersediaan aset ICT terpelihara.	
7.2.3.2	Langkah-langkah yang perlu diambil adalah seperti berikut: a) Mendapatkan kelulusan pegawai bertanggungjawab bagi membawa keluar peralatan ICT; b) Melindungi dan mengawal peralatan ICT sepanjang masa; c) Merekodkan aktiviti peminjaman dan pemulangan peralatan ICT; dan d) Memeriksa peralatan yang dipulangkan berada dalam keadaan baik.	**Pegawai Aset, Pengguna**
7.2.4	**Pengendalian Peralatan ICT Luar Yang Dibawa Masuk Dan Keluar**	
7.2.4.1	Peralatan ICT yang dibawa masuk dari luar bagi tujuan tertentu dan dibawa keluar selepas selesai digunakan hendaklah dipantau bagi memastikan tidak berlaku sebarang kebocoran maklumat.	

7.2.4.2	Langkah keselamatan yang perlu diambil adalah seperti berikut: a) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan; dan b) Memeriksa peralatan yang dibawa keluar bagi mengelak sebarang ketirisan maklumat.	**Pegawai Aset, Pengguna**
7.2.5	**Utilititi Sokongan**	
	Peralatan hendaklah dilindungi daripada kegagalan bekalan kuasa dan gangguan lain yang berpunca dari kegagalan utiliti sokongan.	**Penyedia Perkhidmatan Utiliti**
7.2.5.1	**Bekalan Kuasa**	
	Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi bagi menjamin keselamatan bekalan kuasa adalah seperti berikut: a) Melindungi semua peralatan ICT dari kegagalan bekalan elektrik dengan menyalurkan bekalan yang mencukupi kepada peralatan ICT; b) Memastikan bekalan kuasa berterusan dengan menggunakan peralatan sokongan seperti *Uninterruptible Power Supply (UPS)* atau janakuasa (*power generator*) bagi perkhidmatan kritikal seperti di Pusat Data; dan c) Memeriksa dan menguji semua peralatan sokongan bekalan kuasa secara berjadual.	**Pengurus ICT**
7.2.5.2	**Keselamatan Kabel**	
	Kabel elektrik dan kabel rangkaian hendaklah dilindungi daripada gangguan dan kerosakan. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:	**Pengurus ICT**

	a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c) Melindungi laluan pemasangan kabel sepenuhnya seperti menggunakan *conduit* atau *trunking* mengikut spesifikasi yang ditetapkan bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan d) Membuat pelabelan kabel mengikut spesifikasi dan prosedur yang ditetapkan.	
7.2.6	**Pelupusan dan Guna Semula Peralatan ICT**	
7.2.6.1	Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan yang berkuat kuasa. Pelupusan hendaklah dilakukan secara terkawal dan lengkap. Peralatan ICT yang diguna semula hendaklah dikonfigurasi mengikut spesifikasi asal supaya data sensitif tidak terdedah.	**Pegawai Aset, Pentadbir Sistem dan Pengguna**
7.2.6.2	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua kandungan peralatan ICT hendaklah dihapuskan terlebih dahulu sebelum proses pelupusan dilaksanakan; b) Peralatan ICT yang tidak digunakan dan hendak dilupuskan perlu disimpan di tempat yang telah dikhaskan dan mempunyai ciri-ciri keselamatan; c) Pelupusan peralatan ICT hendaklah dilakukan mengikut tatacara pelupusan semasa yang berkuat kuasa di MinDef; dan d) Pengguna adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:	**Pegawai Aset, Pentadbir Sistem dan Pengguna**

	i. Mengambil mana-mana peralatan ICT atau komponen seperti *memory* dan *hard disk* yang hendak dilupuskan menjadi milik peribadi; dan ii. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan adalah di bawah tanggungjawab jabatan.	
7.2.7	**Polisi *Clear Desk and Clear Screen***	
7.2.7.1	*Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan–bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Pengecualian Polisi *Clear Screen* adalah bagi pentadbir sistem yang terlibat dengan pemantauan masa nyata terhadap prestasi sistem kritikal yang menggunakan paparan di dalam Tempat Larangan.	
7.2.7.2	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Menyimpan bahan yang mengandungi maklumat sensitif mengikut peraturan yang ditetapkan; b) Menggunakan *password screen saver* atau *logout/lock* apabila meninggalkan komputer; dan c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	**Pengguna**
7.3	**Prosedur Kecemasan**	
7.3.1	Prosedur kecemasan merupakan langkah persediaan proaktif untuk melindungi warga MinDef dan pelawat semasa menghadapi bencana seperti kebakaran, banjir dan kemalangan.	**Pegawai Keselamatan Jabatan/ Bahagian, Warga MinDef, Pelawat**

7.3.2	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Warga MinDef dan pelawat hendaklah mematuhi prosedur kecemasan yang ditetapkan; b) Melaporkan insiden kecemasan persekitaran seperti kebakaran kepada Pegawai Keselamatan Jabatan/Bahagian; c) Mewujudkan, menguji dan mengemaskinikan pelan kecemasan dari masa ke semasa; dan d) Mengadakan latihan *fire drill* mengikut jadual.	

BIDANG 8
KESELAMATAN OPERASI

08 KESELAMATAN OPERASI

Memastikan kemudahan pemprosesan maklumat berfungsi dengan cekap dan selamat daripada sebarang ancaman atau gangguan operasi.

Bil	Perkara	Tanggungjawab
8.1	**Prosedur dan Tanggungjawab Operasi**	
	Memastikan pengurusan operasi pemprosesan maklumat dilaksanakan dengan cekap dan selamat.	
8.1.1	**Pengendalian Prosedur Operasi**	
	Semua prosedur pengurusan operasi hendaklah dikenal pasti, didokumenkan, disimpan dan dihadkan capaian berdasarkan keperluan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua prosedur operasi hendaklah didokumenkan dengan jelas, teratur, dikemaskinikan dan sedia diguna pakai oleh pengguna; b) Setiap perubahan kepada prosedur operasi mestilah dikawal; c) Tugas dan tanggungjawab fungsi perlu diasingkan bagi mengurangkan risiko kecuaian dan penyalahgunaan aset ICT MinDef; dan d) Kemudahan ICT untuk kerja-kerja pembangunan, pengujian dan operasi perlu diasingkan bagi mengurangkan risiko capaian atau pengubahsuaian secara tidak sah ke atas sistem yang sedang beroperasi.	**Pengurus ICT, Pentadbir Sistem**

8.1.2	**Pengurusan Perubahan**	
	Perubahan kepada organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang memberi kesan kepada keselamatan maklumat hendaklah dikawal. Pengurusan ke atas perubahan perlu diambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko. Perkara-perkara yang perlu dipatuhi: a) Mewujudkan prosedur pengurusan perubahan; b) Merekodkan semua perubahan yang telah dipersetujui dan dilaksanakan; dan c) Memantau pelaksanaan perubahan.	**Pemilik Sistem, Pentadbir Sistem**
8.1.3	**Pengurusan Kapasiti**	
	Kapasiti sistem ICT hendaklah dirancang, diurus dan dikawal dengan terperinci bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan operasi sistem ICT. Keperluan kapasiti perlu mengambil kira ciri-ciri keselamatan bagi meminimumkan risiko gangguan kepada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	**Pengurus ICT, Pentadbir Sistem**
8.1.4	**Pengasingan Kemudahan Pembangunan, Ujian dan Operasi**	
	Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian ataupun perubahan tidak sah ke atas persekitaran operasi. Perkara–perkara yang perlu dipatuhi: a) Mewujudkan prosedur keperluan sumber bagi penyediaan persekitaran untuk pembangunan, pengujian dan operasi;	**Pengurus ICT, Pentadbir Sistem**

	b) Merekodkan semua penggunaan sumber yang dilaksanakan; dan c) Memantau pelaksanaan penggunaan sumber bagi tujuan perancangan kapasiti.	
8.2	**Perlindungan daripada *Malware***	
8.2.1	Aset ICT perlu dilindungi supaya tidak terdedah kepada kerosakan yang disebabkan oleh kod berbahaya seperti *virus, worm, trojan* dan lain-lain.	
8.2.2	Kawalan pencegahan, pengesanan dan pemulihan untuk melindungi sistem ICT daripada gangguan *malicious code;* Perkara-perkara yang mesti dipatuhi adalah: a) Memasang sistem keselamatan untuk mengesan perisian berbahaya seperti antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS); b) Mengimbas semua perisian dengan antivirus sebelum menggunakannya; c) Mengemaskinikan paten antivirus dari masa ke semasa; d) Memasang dan menggunakan hanya perisian yang tulen; e) Menyemak kandungan sistem ICT secara berkala bagi mengesan aktiviti yang tidak normal seperti manipulasi data tidak sah yang menyebabkan pertambahan, perubahan, kehilangan atau kerosakan maklumat; f) Memasukkan klausa tanggungan ke dalam kontrak yang ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; g) Mewujud dan melaksanakan prosedur jaminan kualiti ke atas	**ICTSO, Pentadbir Sistem, Pengguna**

	semua perisian yang dibangunkan; g) Memberi amaran mengenai ancaman seperti serangan virus terhadap keselamatan aset ICT MinDef; h) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya dari masa ke semasa; i) Melaksanakan Program Kesedaran Pengguna yang bersesuaian; dan j) Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	
8.3	***Backup***	
8.3.1	Memastikan kesinambungan perkhidmatan berjalan lancar.	
8.3.2	Salinan pendua maklumat dan perisian sistem hendaklah disediakan dan diuji secara berkala selaras dengan polisi *backup* bagi tujuan kesinambungan operasi pemprosesan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a) Membuat salinan pendua ke atas semua maklumat dan sistem perisian mengikut jadual yang ditetapkan atau apabila berlaku perubahan versi; b) Menyimpan salinan pendua di lokasi lain yang selamat; dan c) Menguji sistem pendua bagi memastikan ianya dapat beroperasi dengan normal.	**Pentadbir Sistem**
8.4	**Log dan Pemantauan**	
8.4.1	Semua peristiwa dan bukti kewujudan insiden hendaklah direkodkan untuk tujuan jejak audit.	

8.4.2	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap sistem mestilah mempunyai jejak audit; b) Mewujudkan prosedur untuk memantau penggunaan kemudahan memproses maklumat dan dipantau secara berkala; c) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; d) Maklumat log perlu dilindungi daripada sebarang ubahsuai dan capaian yang tidak dibenarkan; e) Sebarang kesalahan, kesilapan atau penyalahgunaan sistem perlu direkodkan, dianalisis dan diambil tindakan sewajarnya; f) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; g) Waktu yang berkaitan dengan sistem pemprosesan maklumat MinDef perlu diselaraskan dengan satu sumber waktu yang piawai; dan h) Sebarang aktiviti tidak sah seperti kecurian maklumat dan pencerobohan hendaklah dilaporkan kepada MinDefCERT.	**ICTSO, Pentadbir Sistem**
8.5	**Pengurusan *Technical Vulnerability***	
8.5.1	Kawalan terhadap sebarang kelemahan teknikal pada perkakasan, sistem pengoperasian dan sistem aplikasi perlu diuruskan secara berkesan, sistematik dan berkala.	

8.5.2	Perkara-perkara yang perlu dipatuhi adalah: a) Mengenal pasti maklumat keterdedahan teknikal sistem yang digunakan; b) Menilai tahap keterdedahan bagi mengenal pasti risiko yang bakal dihadapi; dan c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	**ICTSO, Pentadbir Sistem**

BIDANG 9
KESELAMATAN KOMUNIKASI

09 KESELAMATAN KOMUNIKASI

Memastikan fasiliti rangkaian serta pengaliran maklumat dalam rangkaian dilindungi sepenuhnya.

Bil	Perkara	Tanggungjawab
9.1	**Pengurusan Keselamatan Rangkaian**	
	Keselamatan rangkaian adalah elemen penting dalam memastikan pengaliran maklumat lancar dan sempurna.	
9.1.1	**Kawalan Infrastruktur Rangkaian**	
	Infrastruktur rangkaian hendaklah dirancang, diurus dan dikawal bagi melindungi keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah: a) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berkaitan dengan sistem rangkaian; b) Peralatan keselamatan seperti *firewall* hendaklah dipasang bagi memastikan hak capaian ke atas sistem dapat dilaksanakan seperti ditetapkan; c) Sebarang cubaan menceroboh dan aktiviti yang boleh mengancam sistem dan maklumat MinDef perlu dipantau dan dikesan melalui pemasangan peralatan keselamatan seperti *Intrusion Prevention System (IPS)*; d) Peralatan rangkaian hendaklah diletakkan di lokasi yang bebas dari risiko seperti banjir, gegaran dan habuk; e) Sebarang keperluan penyambungan rangkaian hendaklah melalui proses dan prosedur yang ditetapkan;	**ICTSO, Pengurus ICT, Pentadbir Sistem**

	f) Penggunaan rangkaian tanpa wayar *(wireless)* LAN di MinDef hendaklah mematuhi peraturan yang dikeluarkan oleh pihak berkenaan seperti MAMPU dan Majlis Keselamatan Negara (MKN); dan g) Semua perisian berkaitan rangkaian dan keselamatan seperti *sniffer* atau *network analyzer* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO.	
9.1.2	**Keselamatan Perkhidmatan Rangkaian**	
	Perkhidmatan rangkaian hendaklah dipastikan sentiasa selamat bagi memastikan kerahsiaan, integriti dan ketersediaan maklumat terjamin. Perkara-perkara yang perlu dipatuhi adalah: a) Mekanisme keselamatan, tahap kesediaan perkhidmatan dan keperluan pengurusan perkhidmatan rangkaian hendaklah dikenal pasti dan dinyatakan dalam perjanjian perkhidmatan rangkaian, sama ada perkhidmatan disediakan secara *in-house* ataupun *outsourced*. b) Semua trafik keluar dan masuk hendaklah ditapis oleh peralatan keselamatan di bawah kawalan MinDef; dan c) Sebarang aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam (PKPA) yang berkuat kuasa perlu disekat melalui penggunaan *Web Content Filtering.*	**ICTSO, Pentadbir Sistem, Pengguna**

9.1.3	**Pengasingan Rangkaian**	
	Pengasingan perkhidmatan rangkaian bertujuan meminimumkan risiko capaian tidak sah dan pengubahsuaian yang tidak dibenarkan. Perkara–perkara yang perlu dipatuhi adalah: a) Mengenal pasti fungsi dan tanggungjawab pengguna; b) Mengkonfigurasi hak capaian pengguna mengikut segmen rangkaian berdasarkan keperluan; c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d) Mengemaskinikan hak capaian pengguna dari masa ke semasa mengikut keperluan; dan e) Operasi rangkaian hendaklah diasingkan untuk meminimumkan risiko capaian dan pengubahsuaian yang tidak dibenarkan.	**Pentadbir Sistem**
9.2	**Pemindahan Maklumat**	
	Memastikan keselamatan maklumat terjamin semasa pertukaran maklumat dengan entiti luar.	
9.2.1	**Prosedur Pemindahan Maklumat**	
	Prosedur ini bertujuan untuk mengendali, menyimpan, memindah serta melindungi maklumat daripada didedah tanpa kebenaran atau salah guna serta memastikan keselamatan pemindahan maklumat dengan entiti luar terjamin. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mengehadkan dan menentukan capaian kepada pengguna yang dibenarkan sahaja;	**ICTSO, Pentadbir Sistem, Pengguna**

	b) Mengehadkan pengedaran data untuk tujuan rasmi dan yang dibenarkan sahaja; c) Polisi, prosedur dan kawalan pemindahan maklumat yang formal perlu diwujudkan untuk melindungi pemindahan maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; d) Sebarang pemindahan maklumat di antara MinDef dan agensi lain mestilah dikawal; dan e) Penggunaan perkhidmatan luar seperti aplikasi media sosial dan perkongsian fail untuk pemindahan maklumat rasmi Kerajaan perlu mendapat kelulusan Ketua Jabatan.	
9.2.2	**Perjanjian Mengenai Pemindahan Maklumat**	
	Non-Disclosure Agreements (NDA) perlu diwujudkan bagi memastikan kerahsiaan, integriti dan ketersediaan (CIA) maklumat terpelihara semasa proses pemindahan maklumat dan perisian di antara MinDef dengan agensi luar.	**Ketua Jabatan/ Agensi, Pentadbir Sistem**
9.2.3	**Pengurusan Mesej Elektronik**	
	Maklumat yang dihantar, diterima dan disimpan melalui mel elektronik MinDef perlu dilindungi bagi menghindari capaian atau sebaran maklumat yang tidak dibenarkan. Pengguna layak menerima kemudahan perkhidmatan e-mel dengan kelulusan dari Ketua Jabatan. Perkara yang perlu dipatuhi adalah seperti di **LAMPIRAN B**: **"Etika Penggunaan Internet Dan E-mel MinDef"**.	**Ketua Jabatan/ Agensi, Pentadbir Sistem, Pengguna**

BIDANG 10

PEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM

10 PEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM

Memastikan sistem yang dibangunkan sama ada secara *in-house* atau *outsourced* mempunyai ciri-ciri keselamatan yang ditetapkan.

Bil	Perkara	Tanggungjawab
10.1	**Keperluan Keselamatan Sistem Maklumat**	
	Memastikan keperluan keselamatan diambil kira dalam setiap proses pembangunan sistem maklumat.	
10.1.1	**Analisis Keperluan dan Spesifikasi Keselamatan Maklumat**	
	Pembangunan sistem baharu atau penambahbaikan sistem sedia ada hendaklah mematuhi perkara-perkara berikut: a) Semua sistem yang dibangunkan sama ada secara *in-house* atau *outsourced* hendaklah dikaji supaya mengikut keperluan pengguna dan selaras dengan dasar atau peraturan berkaitan yang berkuat kuasa; b) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang ditetapkan; dan c) Ujian keselamatan hendaklah dilakukan di setiap peringkat pembangunan sistem bagi memastikan integriti data.	**Pentadbir Sistem, Pembekal**
10.1.2	**Keselamatan Perkhidmatan Aplikasi Melalui Rangkaian Awam (*Public Network*)**	

	Maklumat aplikasi yang melalui rangkaian awam hendaklah dilindungi daripada aktiviti tidak sah seperti penipuan, pendedahan maklumat, pengubahsuaian maklumat yang tidak dibenarkan dan pertikaian kontrak. Perkara-perkara yang perlu dipatuhi adalah: a) Identiti pengguna perlu dikenal pasti dan disahkan bagi menentukan tahap capaian maklumat yang dibenarkan; b) Setiap pengguna sistem perlu diberi peranan mengikut skop dan tanggungjawab yang ditetapkan; dan c) Memastikan pembekal diberi penjelasan mengenai keperluan mematuhi kontrak dan peraturan keselamatan yang ditetapkan.	**Pengurus ICT, Pentadbir Sistem, Pembekal**
10.1.3	**Melindungi Perkhidmatan Transaksi Aplikasi**	
10.1.3.1	Maklumat yang terlibat dalam perkhidmatan transaksi hendaklah dilindungi daripada penghantaran yang tidak lengkap, *mis-routing*, pengubahan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan dan duplikasi mesej atau penjanaan semula.	**Pengurus ICT, Pentadbir Sistem**
10.1.3.2	Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara-perkara yang perlu dipatuhi adalah: a) Memperoleh maklumat teknikal keterdedahan sistem maklumat yang digunakan; b) Menilai tahap keterdedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	**Pengurus ICT, Pentadbir Sistem**

10.2	**Keselamatan Dalam Proses Pembangunan Dan Sokongan**	
	Memastikan keseluruhan proses pembangunan dan sokongan sistem maklumat memenuhi keperluan keselamatan yang ditetapkan.	
10.2.1	**Polisi Keselamatan Dalam Pembangunan Sistem**	
	Peraturan pembangunan sistem yang mengambil kira aspek keselamatan maklumat hendaklah diwujudkan dan dilaksanakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mengawal pelaksanaan perubahan menggunakan prosedur kawalan perubahan yang ditetapkan; b) Mengkaji semula dan menguji aplikasi semasa melaksanakan perubahan terutama ke atas sistem aplikasi kritikal yang sedang beroperasi; c) Memastikan sebarang perubahan ke atas pakej perisian adalah terkawal dan terhad kepada keperluan sahaja; d) Memastikan tiada ruang yang boleh menyebabkan berlakunya kebocoran maklumat; dan e) Memantau pembangunan perisian bagi memastikan keperluan keselamatan dipenuhi.	**Pengurus ICT**
10.2.2	**Prosedur Kawalan Perubahan Sistem**	
	Prosedur kawalan perubahan sistem hendaklah diwujudkan bagi mengawal sebarang perubahan ke atas sistem maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, didokumenkan dan disahkan sebelum diguna pakai;	**Pengurus ICT**

	b) Setiap perubahan kepada pengoperasian sistem perlu dikaji semula dan diuji untuk memastikan tiada sebarang masalah yang timbul terhadap operasi dan keselamatan maklumat; dan c) Kawalan perlu dibuat terhadap sebarang perubahan ke atas sistem aplikasi atau pakej perisian bagi memastikan ianya terhad mengikut keperluan sahaja.	
10.2.3	**Kajian Teknikal Perubahan Platform**	
	Sebarang cadangan perubahan platform hendaklah berasaskan kepada kajian teknikal bagi memastikan pengoperasian sistem tidak terjejas. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan sistem aplikasi dan integriti data disemak supaya operasi sistem tidak terjejas apabila perubahan platform dilakukan; b) Perubahan platform hendaklah dimaklumkan kepada pentadbir sistem yang berkaitan bagi membolehkan ujian pengesahan penggunaan sistem dilaksanakan; dan c) Sebarang perubahan hendaklah selari dengan Pelan Kesinambungan Perkhidmatan MinDef.	**Pentadbir Sistem**
10.2.4	**Prinsip Kejuruteraan Sistem Yang Selamat** ***(Secure Information System Engineering Principles)***	
10.2.4.1	Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari masa ke semasa bagi memastikan keberkesanan kepada keselamatan maklumat.	
10.2.4.2	Semua peringkat pembangunan sistem hendaklah mengambil kira prinsip kejuruteraan sistem berikut: a) Asas Keselamatan *(Security Foundation)*	**Pentadbir Sistem**

	Merujuk kepada DKICT dan pekeliling keselamatan ICT berkuat kuasa dalam reka bentuk sesuatu sistem. b) Berasaskan Risiko *(Risk Based)* Mengurangkan risiko ke tahap boleh terima. c) Mudah Diguna *(Ease of Use)* Mempunyai ciri-ciri open standard untuk *portability* dan *interoperability.* d) Meningkatkan Daya Tahan *(Increase Resilience)* Memastikan tiada sebarang kelemahan melalui pelaksanaan keselamatan *(layered security).* e) Mengurang Kelemahan *(Reduce Vulnerabilities)* Meminimumkan kelemahan disebabkan reka bentuk yang kompleks supaya penyenggaraan sistem mudah dilaksanakan. f) Mengambil kira Keperluan Rangkaian dalam Reka Bentuk Sistem *(Design with Network in Mind)* Pelaksanaan keselamatan hendaklah mengambil kira capaian sistem daripada dalam dan luar premis.	
10.2.5	**Persekitaran Pembangunan Sistem Yang Selamat**	
	Persekitaran bagi pembangunan sistem hendaklah selamat untuk melindungi keseluruhan proses pembangunan sistem (*development life cycle*). Secara umumnya, tiga (3) persekitaran sistem perlu diwujudkan iaitu Persekitaran Pembangunan (*Development Environment*), Persekitaran Ujian (*Testing Environment*), dan Persekitaran Operasi (*Production Environment)* bagi memastikan kelancaran operasi.	**Pentadbir Sistem**

10.2.6	**Pembangunan Sistem Secara *Outsource***	
	Pembangunan sistem secara *outsource* perlu dikawal selia dan dipantau. *Intellectual property rights (IPR)* dan kod sumber (*source code)* hendaklah menjadi hak milik Kerajaan.	**Pentadbir Sistem**
10.2.7	**Ujian Keselamatan Sistem**	
	Ujian keselamatan sistem hendaklah dijalankan ke atas tiga (3) peringkat pemprosesan maklumat iaitu peringkat kemasukan data (*input*), peringkat pemprosesan data (*process*), dan peringkat penjanaan laporan (*output*). Perkara–perkara yang perlu dipatuhi oleh pentadbir sistem adalah: a) Merancang dan melaksanakan penilaian risiko mengikut keperluan bagi mengenal pasti dan melaksana kawalan yang sesuai bagi pengesahan dan perlindungan integriti data dalam aplikasi; b) Merancang dan melaksana *Security Posture Assessment* (SPA) bagi mengenal pasti kelemahan sistem; dan c) Membuat semakan pengesahan sistem aplikasi untuk mengenal pasti sebarang pencemaran maklumat sama ada disebabkan oleh kesilapan atau disengajakan.	**Pentadbir Sistem**
10.2.8	**Pengujian Penerimaan Sistem**	
	Program Pengujian Penerimaan Sistem (Ujian Penerimaan Pengguna dan Ujian Penerimaan Akhir) hendaklah dilaksanakan berdasarkan kriteria yang telah ditetapkan sebelum sistem diguna pakai.	**Pentadbir Sistem, Pengguna, Pembekal**

10.3	**Data Ujian**	
	Data ujian hendaklah disediakan dengan secukupnya sebelum ujian dilaksanakan. Perkara–perkara yang perlu dipatuhi adalah: a) Data ujian yang hendak digunakan perlu dipilih, dilindungi dan dikawal. b) Mengaktifkan audit log bagi merekodkan semua aktiviti pengujian dan pengemaskinian untuk tujuan statistik, pemulihan, keselamatan dan pengesahan data.	**Pentadbir Sistem, Pengguna**

BIDANG 11
HUBUNGAN DENGAN PEMBEKAL

11 HUBUNGAN DENGAN PEMBEKAL

Memastikan aset ICT MinDef dilindungi sepenuhnya daripada akses yang tidak sewajarnya oleh pembekal.

Bil	Perkara	Tanggungjawab
11.1	**Keselamatan Maklumat Dalam Hubungan Dengan Pembekal**	
11.1.1	**Polisi Keselamatan Maklumat Ke Atas Pembekal**	
	Semua pembekal adalah tertakluk kepada Dasar Keselamatan Kerajaan yang berkuat kuasa. Perkara–perkara yang perlu dipatuhi adalah seperti berikut: a) Pembekal hendaklah menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MinDef; dan b) Pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas.	**Pengurus ICT, Pembekal**
11.1.2	**Kawalan Keselamatan Maklumat Melalui Perjanjian Dengan Pembekal**	
	Semua keperluan keselamatan maklumat yang berkaitan hendaklah diguna pakai bagi tujuan mengakses, memproses, menyimpan, berkomunikasi dan menyediakan komponen infrastruktur ICT.	**Pengurus ICT, Pembekal**
11.1.3	**Kawalan Keselamatan Maklumat Dengan Pembekal Dan Pihak Ketiga**	
	Perjanjian dengan pembekal hendaklah meliputi risiko keselamatan yang merangkumi perkhidmatan ICT dengan pihak ketiga.	**Pengurus ICT, Pembekal**

11.2	**Pengurusan Penyampaian Perkhidmatan Pembekal**	
11.2.1	**Pemantauan dan Kajian Perkhidmatan Pembekal**	
	Prestasi perkhidmatan pembekal hendaklah sentiasa dipantau, diaudit dan dikaji semula secara berkala.	**Pentadbir Sistem**
11.2.2	**Pengurusan Perubahan Perkhidmatan Pembekal**	
	Semua perubahan perkhidmatan pembekal hendaklah dilaksanakan secara teratur dan mengikut SOP yang ditetapkan. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a) Perubahan dalam perjanjian dengan pembekal; b) Perubahan yang dilakukan oleh MinDef bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan c) Perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	**Pengurus ICT**

BIDANG 12

PENGURUSAN INSIDEN KESELAMATAN ICT

12 PENGURUSAN INSIDEN KESELAMATAN ICT

Memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, tepat dan berkesan bagi memastikan perkhidmatan ICT MinDef dapat beroperasi semula.

Bil	Perkara	Tanggungjawab
12.1	**Prosedur Pengurusan Insiden Keselamatan ICT**	
12.1.1	Prosedur bagi mengurus insiden keselamatan ICT perlu diwujudkan dan didokumenkan. MinDefCERT/MAFCERT bertanggungjawab dalam pengurusan pengendalian insiden keselamatan ICT berpandukan prosedur operasi standard (SOP) keselamatan ICT MinDef.	**MinDefCERT/ MAFCERT**
12.1.2	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mematuhi Pelan Pemulihan Bencana ICT MinDef seperti yang telah digariskan dalam Pelan Kesinambungan Perkhidmatan MinDef; b) Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; c) Menyimpan jejak audit dan memelihara bahan bukti; dan d) Menyediakan dan melaksanakan pelan tindakan pemulihan.	**MinDefCERT/ MAFCERT**
12.1.3	Insiden keselamatan ICT adalah meliputi perkara-perkara berikut: a) Maklumat didapati atau disyaki hilang (serangan virus, kecurian dan lain-lain); b) Maklumat didedahkan kepada pihak yang tidak diberi kuasa;	**MinDefCERT/ MAFCERT**

	c) Sistem maklumat disyaki digunakan tanpa kebenaran; d) Kecurian data dan maklumat; e) Mekanisme kawalan akses seperti kata laluan dikompromi; f) Sistem beroperasi secara tidak normal seperti kehilangan maklumat, kegagalan fungsi sistem atau ralat dalam komunikasi data; dan g) Berlaku pencerobohan dan penyelewengan data.	
12.1.4	Pelaporan insiden keselamatan ICT berdasarkan kepada pekeliling yang berkuat kuasa termasuk: a) Pekeliling Am Bilangan 1 Tahun 2001 bertajuk ”Mekanisme Pelaporan Insiden Keselamatan ICT”. b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	**MinDefCERT/ MAFCERT**
12.2	**Mekanisme Pelaporan Insiden Keselamatan ICT**	
12.2.1	**Pelaporan Insiden**	
	Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada MinDefCERT/MAFCERT dengan segera supaya siasatan dan tindakan pemulihan dapat dilakukan. Semua maklumat adalah sulit dan hanya boleh didedahkan kepada pihak yang dibenarkan sahaja.	**Warga MinDef, MinDefCERT/ MAFCERT**
12.2.2	**Pelantikan Pegawai Bertanggungjawab**	
	Pegawai Keselamatan ICT (ICTSO) dan anggota MinDefCERT/ MAFCERT hendaklah dilantik secara rasmi dan dimaklumkan kepada warga MinDef.	**Ketua Jabatan, CIO**

12.3	**Pengurusan Maklumat Insiden Keselamatan ICT**	
12.3.1	Maklumat mengenai insiden keselamatan ICT perlu dikumpul, dianalisis dan disimpan bagi tujuan perancangan dan tindakan untuk melaksanakan peningkatan dan kawalan tambahan.	**MinDefCERT / MAFCERT**
12.3.2	MinDefCERT/MAFCERT hendaklah memastikan bahan bukti berkaitan insiden keselamatan ICT dapat disediakan, disimpan, disenggarakan dan mempunyai perlindungan keselamatan. Penyediaan bahan bukti seperti jejak audit, *backup* berkala dan *off-site backup* hendaklah mengikut tatacara perundangan yang berkuat kuasa.	**MinDefCERT / MAFCERT**
12.3.3	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Melindungi integriti bahan bukti; b) Mengumpul dan menyimpan bahan bukti bagi tujuan analisis; c) Merekodkan semua maklumat insiden termasuk maklumat pegawai yang terlibat, perisian, perkakasan dan peralatan yang digunakan; d) Memaklumkan kepada pihak berkuasa perundangan, seperti pegawai undang undang dan polis (jika perlu); e) Mendapatkan nasihat dari pihak berkuasa perundangan ke atas bahan bukti yang diperlukan (jika perlu); dan f) Menyediakan laporan insiden kepada CIO.	**MinDefCERT / MAFCERT**
12.4	**Pengurusan Insiden Keselamatan Aset Bukan ICT**	
	Insiden keselamatan aset bukan ICT penting untuk dipantau kerana insiden ini boleh menjadi permulaan kepada insiden keselamatan aset ICT. Rujuk Arahan Jawatankuasa Induk Keselamatan MinDef.	**Warga MinDef**

BIDANG 13

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

13 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Memastikan aspek keselamatan maklumat diberi penekanan dalam Pelan Kesinambungan Perkhidmatan bagi menjamin operasi perkhidmatan yang berterusan kepada pengguna.

Bil	Perkara	Tanggungjawab
13.1	**Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan**	
13.1.1	**Perancangan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan**	
	Aspek keselamatan maklumat hendaklah menjadi elemen penting dalam pembangunan Pelan Kesinambungan Perkhidmatan MinDef bagi memastikan perkhidmatan MinDef tidak terganggu semasa krisis atau bencana.	**ICTSO**
13.1.2	**Pelaksanaan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan**	
	Prosedur berkaitan pelaksanaan keselamatan maklumat hendaklah diwujudkan, didokumenkan, dilaksanakan dan dikemaskinikan bagi memastikan keselamatan maklumat berada di tahap yang ditetapkan semasa krisis atau bencana. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mengenal pasti tanggungjawab ketika berlaku kecemasan dan pemulihan; b) Melaksanakan prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;	**Pengurus ICT**

	c) Mengenal pasti perkara-perkara yang boleh mengakibatkan gangguan terhadap proses bisnes MinDef serta impak ke atas keselamatan ICT; d) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; e) Membuat *backup*; dan f) Menguji dan mengemaskinikan pelan sekurang-kurangnya setahun sekali.	
13.1.3	**Pelaksanaan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan *(Review)***	
	Kawalan berkaitan prosedur pelaksanaan keselamatan maklumat hendaklah dikaji semula, dinilai dan dilaksanakan secara berkala bagi memastikan ianya sah dan berkesan semasa krisis atau bencana.	**Pengurus ICT**
13.2	***Redundancy***	
13.2.1	**Ketersediaan Kemudahan Pemprosesan Maklumat**	
	Semua sistem aplikasi yang kritikal hendaklah mempunyai kemudahan *redundancy* dan diuji (*failover test*) keberkesanannya dari masa ke semasa.	**Pengurus ICT, Pentadbir Sistem**

BIDANG 14
PEMATUHAN

14 PEMATUHAN

Meningkatkan tahap kesedaran dan keselamatan ICT bagi mencegah pelanggaran Dasar Keselamatan ICT MinDef (DKICT).

Memantapkan keselamatan maklumat bagi mengelak berlaku sebarang pelanggaran undang-undang, statutori, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.

Bil	Perkara	Tanggungjawab
14.1	**Pematuhan Dasar**	
14.1.1	Setiap warga MinDef hendaklah membaca, memahami dan mematuhi DKICT, undang-undang dan peraturan-peraturan lain yang berkuat kuasa.	**Warga MinDef**
14.1.2	ICTSO bertanggungjawab dan berhak memantau aktiviti pengguna untuk mengesan penggunaan aset ICT MinDef bagi tujuan selain dari yang telah ditetapkan.	**ICTSO**
14.2	**Pematuhan Terhadap Keperluan Perundangan dan Obligasi Kontrak**	
	Senarai undang-undang, peraturan dan kontrak yang berkaitan dengan MinDef perlu dikenal pasti, didokumenkan, disimpan dan dikemaskinikan.	
14.2.1	**Mengenal Pasti Undang-Undang dan Perjanjian Kontrak**	
	Keperluan perundangan perlu dipatuhi berdasarkan kepada peraturan-peraturan yang telah ditetapkan. Berikut adalah keperluan perundangan atau peraturan-peraturan lain yang perlu dipatuhi oleh semua pengguna:	**Warga MinDef**

	a) Arahan Keselamatan; b) Perintah Am Angkatan Tentera (PAAT); c) Akta Tanda Tangan Digital 1997; d) Akta Jenayah Komputer 1997; e) Akta Hak cipta (Pindaan) Tahun 1997; f) Akta Komunikasi dan Multimedia 1998; g) Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan"; h) Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)"; i) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"; j) *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS); dan k) Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; l) Surat MAMPU dengan rujukan UPTM (S) 159/338/8 Jilid 30 (84) bertajuk "Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) di Agensi-agensi Kerajaan".	
14.2.2	**Hak Harta Intelek *(Intellectual Property Rights)***	
	Prosedur pengawalan hendaklah dilaksanakan bagi memastikan pematuhan kepada perundangan, peraturan dan keperluan kontrak	**Pengurus ICT**

	berkaitan produk yang mempunyai IPR termasuk perisian *proprietary*.	
14.2.3	**Perlindungan Rekod**	
	Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian dan pengeluaran yang tidak sah mengikut undang-undang, peraturan, kontrak dan keperluan MinDef.	**Ketua Jabatan**
14.2.4	**Privasi dan Perlindungan Maklumat Peribadi**	
	Maklumat peribadi dan privasi pengguna hendaklah dilindungi seperti yang tertakluk dalam undang-undang kerajaan Malaysia dan peraturan-peraturan yang berkaitan.	**Ketua Jabatan, Pembekal**
14.2.5	**Peraturan Kawalan Kriptografi**	
	Kawalan kriptografi hendaklah dilaksanakan berdasarkan kepada perjanjian kontrak, undang-undang dan peraturan-peraturan berkaitan.	**Pengurus ICT**
14.2.6	**Perlanggaran Perundangan**	
	Pelanggaran dasar ini boleh dikenakan tindakan undang-undang dan tatatertib di bawah Akta Rahsia Rasmi 1972 dan Perintah-Perintah Am Bab "D"– Peraturan-peraturan Pegawai Awam (Kelakuan Dan Tatatertib).	**Warga MinDef**
14.3	**Kajian Semula Keselamatan Maklumat**	
	Memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur yang ditetapkan.	
14.3.1	**Kajian Bebas/Pihak Ketiga Terhadap Keselamatan Maklumat**	
	Pelaksanaan prosedur keselamatan maklumat hendaklah dikaji secara bebas atau oleh pihak ketiga dari masa ke semasa atau	**Ketua Jabatan**

	apabila terdapat perubahan yang signifikan prosedur keselamatan maklumat.	
14.3.2	**Pematuhan Kepada Dasar, Standard Dan Teknikal Keselamatan**	
14.3.2.1	Dasar ini bertujuan memastikan keselamatan maklumat disemak secara berkala supaya patuh dan selaras dengan dasar dan standard keselamatan Mindef.	**ICTSO**
14.3.2.2	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pegawai penyelia hendaklah memastikan bahawa semua peraturan keselamatan dikawal selia dan dipatuhi selaras dengan perundangan, peraturan dan lain-lain keperluan keselamatan; b) Sistem maklumat hendaklah disemak dan diuji secara berkala untuk memastikan pematuhan pelaksanaan standard keselamatan yang ditetapkan; c) ICTSO perlu memastikan semua prosedur keselamatan mematuhi dasar, standard dan keperluan teknikal; dan d) Sebarang penilaian pematuhan teknikal seperti aktiviti *Security Posture Assessment* (SPA) mestilah dijalankan oleh individu yang kompeten dan dibenarkan.	**ICTSO,** **Pengurus ICT**
14.3.3	**Kajian Semula Pematuhan Teknikal**	
	Pematuhan teknikal ke atas sistem maklumat hendaklah dikaji semula selaras dengan pematuhan dasar dan standard keselamatan maklumat sekurang-kurangnya dua (2) tahun sekali atau mengikut keperluan.	**Pengurus ICT dan Pentadbir Sistem**

GLOSARI

TERMINOLOGI	MAKSUD
Arahan Keselamatan	Panduan mengenai peraturan-peraturan keselamatan yang perlu dipatuhi oleh semua kakitangan kerajaan.
Aset ICT	Komponen-komponen yang terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Bahagian Staf Perisikan Pertahanan (BSPP)	Bahagian yang mengendalikan tugas-tugas perisikan Angkatan Tentera Malaysia, bertanggungjawab terus kepada Panglima Angkatan Tentera.
Central Processing Unit (CPU)	Perkakasan yang terdiri daripada *processor, hard disk, memory* dan *motherboard.*
Chief Information Officer (CIO)	Pegawai yang dilantik dan bertanggungjawab ke atas pengurusan maklumat organisasi.
Clear Desk and Clear Screen	Konsep tidak meninggalkan sebarang maklumat sama ada atas meja atau di paparan skrin apabila pengguna tidak berada di tempatnya.
Enkripsi	Kaedah pertukaran format data daripada bentuk asal kepada bentuk lain menggunakan algoritma tertentu.
Firewall	Peralatan dalam bentuk perkakasan dan perisian untuk mencegah capaian ke atas maklumat pada server atau rangkaian oleh pengguna yang tidak dibenarkan.
Intrusion Detection System (IDS)	Satu peralatan yang digunakan untuk memantau atau merekod cubaan pencerobohan.

TERMINOLOGI	MAKSUD
Jawatankuasa Pemandu ICT MinDef	Jawatankuasa tertinggi di peringkat Kementerian Pertahanan yang dipengerusikan oleh KSU/CIO dan dianggotai oleh Ketua Jabatan/ Bahagian/Perkhidmatan ATM. Jawatankuasa ini berperanan meluluskan dan menguatkuasakan dasar, hala tuju, garis panduan dan standard keselamatan ICT.
Jawatankuasa Teknikal ICT MinDef	Jawatankuasa yang bertanggungjawab ke atas penilaian keupayaan teknikal dan keselamatan sesuatu projek ICT.
Jejak Audit *(Audit Trail)*	Satu proses untuk mengenal pasti semua aktiviti yang dilakukan oleh komputer dalam memproses kemasukan data, penjanaan output dan segala aktiviti yang terlibat di antaranya.
Kata laluan	Satu gabungan antara huruf dan nombor atau aksara khusus untuk mengesahkan pengenalan diri bagi capaian kepada sesuatu sistem.
Ketua Jabatan	Pegawai awam atau tentera yang mengetuai sesebuah Jabatan/ Bahagian/Perkhidmatan ATM.
Kriptografi	Proses penukaran format maklumat asal kepada format maklumat yang hanya boleh difahami menggunakan fungsi tertentu.
Media Storan	Peralatan untuk menyimpan maklumat digital.
Mel Elektronik	Mel yang dihantar secara elektronik.
MinDefCERT/MAFCERT	Pasukan yang bertanggungjawab dan bertindak apabila berlaku insiden keselamatan ICT di MinDef.
Outsource	Menggunakan khidmat nasihat dari konsultan luar bagi melaksanakan projek-projek ICT disebabkan kekurangan kemahiran dan sumber manusia.

TERMINOLOGI	MAKSUD
Pembekal	Individu atau kumpulan yang menyediakan perkhidmatan ICT kepada MinDef.
Pegawai Keselamatan ICT (ICTSO)	Pegawai yang bertanggungjawab untuk menjaga keselamatan ICT.
Pegawai Keselamatan Maklumat Jabatan/ Bahagian/Perkhidmatan ATM	Pegawai yang dilantik dan bertanggungjawab ke atas keselamatan maklumat Jabatan/Bahagian/Perkhidmatan ATM.
Pelan Kesinambungan Perkhidmatan (PKP)	Pelan tindakan yang menyeluruh bagi memastikan kesinambungan perkhidmatan dapat diteruskan apabila berlaku bencana.
Pengesahan *(Authentication)*	Kaedah untuk mengesahkan identiti pengguna, peralatan, atau entiti dalam sistem komputer sebelum kebenaran akses kepada sesuatu sistem diberikan.
Pengguna	Semua warga MinDef yang menggunakan perkhidmatan ICT yang disediakan oleh Jabatan/Bahagian/Perkhidmatan ATM.
Pengurus ICT	Ketua ICT Jabatan/Bahagian/Perkhidmatan ATM.
Pentadbir Sistem	Pegawai yang bertanggungjawab untuk menjalankan tugas-tugas pembangunan, penyelenggaraan dan pentadbiran sesuatu sistem ICT.
Perkakasan	Semua aset yang digunakan untuk menyokong pemprosesan dan penyimpanan maklumat digital MinDef seperti komputer, *server* dan peralatan komunikasi.
Perisian	Bahagian sistem komputer yang berfungsi menjalankan sistem, dan terdiri daripada cara, rutin, subrutin dan suruhan yang ditulis dalam bahasa pengaturcaraan. Penghimpun, penyusun, penjana dan sistem pengendalian digolongkan sebagai perisian.

TERMINOLOGI	MAKSUD
Rangkaian MinDef	Semua rangkaian yang diwujudkan khusus untuk kegunaan dan di bawah kawalan MinDef.
Telecommuting	Merupakan satu cara yang membolehkan pegawai untuk melaksanakan tugas di mana sahaja dan dalam masa yang sama berhubung secara terus *(Online)* dengan pejabat.
Uninterruptible Power Supply (UPS)	Peranti mengandungi bateri untuk menyimpan kuasa yang bertujuan untuk mengambil alih peranan kuasa elektrik sekiranya berlaku gangguan bekalan kuasa.
Warga MinDef	Semua pegawai dan kakitangan Kementerian Pertahanan termasuk awam dan tentera.

LAMPIRAN

LAMPIRAN A

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT MINDEF

Nama : .....

No. KP / Tentera : .....

Jawatan / Pangkat : .....

Jabatan / Bahagian / Perkhidmatan ATM / 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 MinDef.
2. Sekiranya saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan undang-undang boleh diambil ke atas diri saya.

.....

(Tandatangan)

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT (ICTSO) Cop Jabatan

.....

Tarikh : .....

ETIKA PENGGUNAAN INTERNET
DAN
E-MEL KEMENTERIAN PERTAHANAN

A ETIKA PENGGUNAAN INTERNET

1. Capaian Internet hendaklah menggunakan terminal yang dikhaskan untuk Internet sahaja dan dilengkapi dengan ciri-ciri sistem keselamatan.

2. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan.

3. Melayari laman web yang menentang pemerintahan kerajaan, berunsur hasutan dan mempunyai unsur-unsur lucah adalah dilarang sama sekali.

4. Pengguna hendaklah memastikan ketepatan dan kesahihan bahan yang diperolehi dari Internet.

5. Rujukan yang didapati daripada sumber Internet hendaklah dinyatakan dengan jelas.

6. Bahan rasmi yang hendak dimuat naik ke Internet hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik.

7. Tindakan memuat turun hanya dibenarkan ke atas bahan yang sah seperti perisian yang berdaftar di bawah hak cipta terpelihara.

8. Pengguna hendaklah memastikan sebarang bahan yang dimuat turun dari Internet mestilah bebas daripada kod perosak (virus, *worm, trojan horse* dan *trap door*).

9. Bahan yang dimuat turun hendaklah digunakan untuk tujuan yang dibenarkan oleh jabatan sahaja.

10. Kandungan perbincangan awam seperti *newsgroup* dan *bulletin board* mestilah mendapat pengesahan daripada Ketua Jabatan tertakluk kepada dasar dan tatacara yang telah ditetapkan.

11. Pengguna yang memasuki perbincangan awam adalah bertanggunjawab untuk mengekalkan konsistensi dan keutuhan maklumat yang dikongsi.

12. Pengguna adalah **DILARANG** daripada memuat naik, memuat turun dan menyimpan gambar atau teks yang bercorak penentangan yang boleh membawa keadaan huru-hara dan menakutkan pengguna Internet yang lain.

13. Pengguna adalah **DILARANG** daripada memuat turun, menyimpan dan menggunakan perisian berbentuk hiburan atas talian seperti permainan elektronik, video dan lagu.

14. Pengguna adalah **DILARANG** untuk menggunakan kemudahan *chatting* melalui Internet.

15. Pengguna adalah **DILARANG** daripada menyedia dan menghantar maklumat berulang-ulang yang berupa gangguan.

RUJUKAN

1. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003

B ETIKA PENGGUNAAN E-MEL RASMI (@mod.gov.my)

1. Semua warga MinDef disediakan kemudahan e-mel mengikut keperluan tugas dengan kelulusan dari Ketua Jabatan.

2. Alamat e-mel hendaklah berdasarkan *naming convention* yang telah ditetapkan iaitu berdasarkan nama pemohon dan jika ada persamaan nama, nama bapa akan ditambah pada nama dan dipisahkan oleh titik (dot).

3. Penggunaan akaun e-mel hanya untuk urusan rasmi sahaja.

4. Maklumat terperingkat adalah tidak dibenarkan sama sekali dihantar melalui e-mel.

5. Saiz e-mel termasuk e-mel yang mengandungi fail lampiran yang dihantar atau diterima hanya dibenarkan sehingga 10 megabait. Kaedah pemampatan untuk mengurangkan saiz fail adalah disarankan.

6. Semua e-mel lama hendaklah diarkibkan dalam media storan untuk simpanan dan rujukan masa hadapan.

7. Semua e-mel yang telah selesai diambil tindakan hendaklah dihapuskan selepas disimpan dalam storan kedua dan diarkibkan.

8. Pengguna hendaklah memastikan e-mel yang diterima bebas daripada kod perosak (virus, *worm, trojan horse* dan *trap door*).

9. E-mel yang diragui atau tidak dikenali hendaklah dihapuskan dengan segera.

10. Pengguna adalah bertanggungjawab untuk melaporkan kepada Pentadbir Sistem E-mel di BPM apabila menerima e-mel yang meragukan atau tidak dikenali.

11. Pengguna adalah **DILARANG** untuk menggunakan akaun e-mel milik orang lain.

12. Pengguna adalah **DILARANG** untuk menyamar sebagai penghantar maklumat yang sah.

13. Pengguna adalah **DILARANG** daripada menyebarkan kod perosak (virus, *worm, trojan horse* dan *trap door*) yang boleh merosakkan sistem komputer dan maklumat pengguna

14. Pengguna adalah **DILARANG** daripada membenarkan pihak lain untuk menjawab e-mel kepada penghantar asal bagi pihaknya

15. Pentadbir Sistem E-mel berhak memantau dan mengakses akaun e-mel atas sebab-sebab kepentingan kementerian.

RUJUKAN

1. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003

BRING YOUR OWN DEVICE (BYOD)

BYOD adalah peralatan mudah alih persendirian seperti telefon pintar, *tablet* dan *laptop* yang digunakan untuk tujuan rasmi. Walaupun fenomena ini berupaya meningkatkan produktiviti, penggunaan peralatan mudah alih di tempat kerja boleh menimbulkan risiko besar kepada keselamatan maklumat jika tidak mempunyai strategi untuk menangani vektor ancaman baru ini.

Bagi kebanyakan organisasi, menyekat penggunaan peralatan mudah alih peribadi adalah pilihan yang tidak realistik. Realiti bisnes masa kini terus menekan dan memaksa pengurusan organisasi untuk membenarkan penggunaan peralatan mudah alih peribadi bagi mencapai aplikasi dan data rasmi organisasi, walaupun risiko yang bakal dihadapi adalah tinggi, tetapi risiko ini perlu diuruskan dengan sebaiknya.

Risiko keselamatan melibatkan peralatan mudah alih peribadi boleh dibahagikan kepada dua kategori iaitu risiko alat dan risiko aplikasi.

a) **Risiko Alat** berpunca daripada peralatan mudah alih peribadi berkeupayaan tinggi seperti penyimpanan data sama ada dalaman atau di *cloud*, penghantaran maklumat keluar daripada organisasi dan kehilangan peralatan. Organisasi biasanya tidak mempunyai kawalan atau mempunyai kawalan yang sangat terhad terhadap peralatan mudah alih ini berbanding *PC desktop* atau komputer riba yang dibekalkan.

b) **Risiko Aplikasi** timbul akibat daripada pekerja memasang aplikasi mudah alih pihak ketiga yang berinteraksi dengan data rasmi organisasi yang disimpan di dalam peralatan.

EMPAT LANGKAH MEMASTIKAN KESELAMATAN PENGGUNAAN PERALATAN MUDAH ALIH PERIBADI

LANGKAH 1

Kurangkan Risiko dengan Pengurusan Peralatan Mudah Alih *(Mobile Device Management)*

a) Organisasi tidak mempunyai kawalan terhadap telefon pintar dan tablet peribadi. Pertukaran dan penggantian peralatan mudah alih peribadi adalah hak warga MinDef, walau bagaimanapun data yang disimpan dan dihantar keluar dari organisasi melibatkan data rasmi organisasi. Terdapat potensi ancaman yang besar seperti kehilangan data apabila berlaku insiden seperti kehilangan telefon pintar atau tablet. Langkah yang perlu diambil adalah dengan mengenal pasti dan mendaftar peralatan mudah alih yang dibenarkan untuk mencapai data rasmi organisasi.

b) Maklumat rasmi perlu dibuat pengelasan dan peralatan mudah alih yang dibenarkan untuk mencapai maklumat dan aplikasi mengikut pengelasan berkaitan perlu ditentukan.

c) Penggunaan *tool* Pengurusan Peralatan Mudah Alih boleh membantu memudahkan pengurusan berikut:

- Konfigurasi telefon pintar dan tablet
- Agihan dan capaian perisian/aplikasi
- Enkripsi dan pengurusan kata laluan
- *Remote wipe and lock*

LANGKAH 2

Kurangkan Risiko Muat Turun Aplikasi Melalui Polisi dan Latihan

a) Aplikasi yang dimuat turun oleh warga MinDef melalui Internet ke dalam telefon pintar dan tablet boleh mendatangkan ancaman dan risiko serta impak yang besar terhadap keselamatan apabila peranti yang sama digunakan untuk mencapai maklumat dan aplikasi rasmi MinDef. Sukar untuk mewujudkan kawalan terhadap aplikasi yang dimuat turun dan kebanyakan aplikasi yang dimuat turun daripada sumber yang tidak diketahui berkemungkinan mengandungi *malicious code.*

b) Sesetengah aplikasi yang dimuat turun mempunyai keupayaan untuk memuat naik maklumat dan gambar yang disimpan dalam peranti pintar peribadi secara sulit dan tidak diketahui oleh pemiliknya. Pembekal peranti pintar seperti Apple IOS atau Android belum mempunyai kaedah khusus untuk menyekat ancaman ini daripada berlaku.

c) Bagi warga MinDef yang diberi kebenaran menggunakan telefon pintar dan tablet peribadi untuk mencapai maklumat rasmi MinDef, muat turun aplikasi perlu dibuat melalui sumber yang dipercayai *(trusted AppStore).*

LANGKAH 3

Menbangunkan Aplikasi Secara Dalaman

a) Banyak organisasi telah mula membangunkan aplikasi peralatan mudah alih secara dalaman sebagai salah satu saluran komunikasi dan melaksanakan bisnes dengan pelanggan dan pengguna.

b) Aplikasi yang dibangunkan ini menyediakan kaedah autentikasi sebelum capaian kepada data organisasi dibenarkan.

c) Pembangunan aplikasi secara dalaman ini merupakan salah satu langkah pilihan daripada membenarkan warga MinDef memuat turun aplikasi daripada sumber yang tidak dipercayai.

d) Walau bagaimanapun aplikasi yang dibangunkan perlu mematuhi metodologi pembangunan sistem secara selamat.

LANGKAH 4

Melaksanakan Audit Keselamatan Terhadap Peralatan, Infrastruktur dan Aplikasi Mudah Alih

a) Tidak ada sebarang strategi keselamatan peralatan mudah alih yang komprehensif melainkan setelah audit keselamatan terhadap peralatan, infrastruktur dan aplikasi dilaksanakan.

b) Pelaksanaan audit keselamatan perlu meliputi aspek berikut:

- Membuat penilaian terhadap infrastruktur ICT mudah alih;
- Melaksanakan ujian penembusan (*penetration test*) terhadap peralatan mudah alih dan server yang terlibat;
- Membuat penilaian terhadap keselamatan aplikasi bagi menentukan jika terdapat kemungkinan berlaku kebocoran maklumat; dan
- Menilai jurang antara polisi dan prosedur yang dikuat kuasa dengan amalan terbaik (*best practices*).

RUJUKAN

1. Akta Aktiviti Kerajaan Elektronik 2007 (AKTA 680),
2. Akta Tandatangan Digital 1997,
3. Arahan Keselamatan,
4. Arahan Teknologi Maklumat,
5. Pekeliling Am Bil. 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan,
6. Pekeliling Am Bil. 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi(ICT),
7. Pekeliling Perkhidmatan Bil. 5 Tahun 2007 - Panduan Pengurusan Pejabat,
8. Surat Pekeliling Am Bil. 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam,
9. Perintah Am Angkatan Tentera Bil. 1/2013 - Pencegahan Pencemaran Maklumat ATM melalui Platform Siber,
10. Perintah Am Angkatan Tentera Bil. 3/2013 - Garis Panduan Media Sosial ATM,
11. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 - Garis Panduan Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan,
12. Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bil. 3 Tahun 2015 - Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan,
13. Surat Arahan Ketua Setiausaha Negara bertarikh 20 October 2006 - Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network)* di Agensi– Agensi Kerajaan, Handbook (MyMIS),

14. *Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMIS),*
15. Polisi Kawalan Akses (*Access Control Policy),*
16. Dasar Kriptografi Negara,
17. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) versi 1.0,
18. *MS ISO/IEC 27001 Information Security Management System,*
19. 1Pekeliling Perbendaharaan (1PP): Tatacara Pengurusan Aset Alih Kerajaan.

DISEDIAKAN OLEH

BAHAGIAN PENGURUSAN MAKLUMAT
KEMENTERIAN PERTAHANAN MALAYSIA
WISMA PERTAHANAN, JALAN PADANG TEMBAK
50634, KUALA LUMPUR