KEMENTERIAN PERTAHANAN

POLISI KESELAMATAN SIBER

VERSI 1.0

ISBN 978-967-26651-1-3

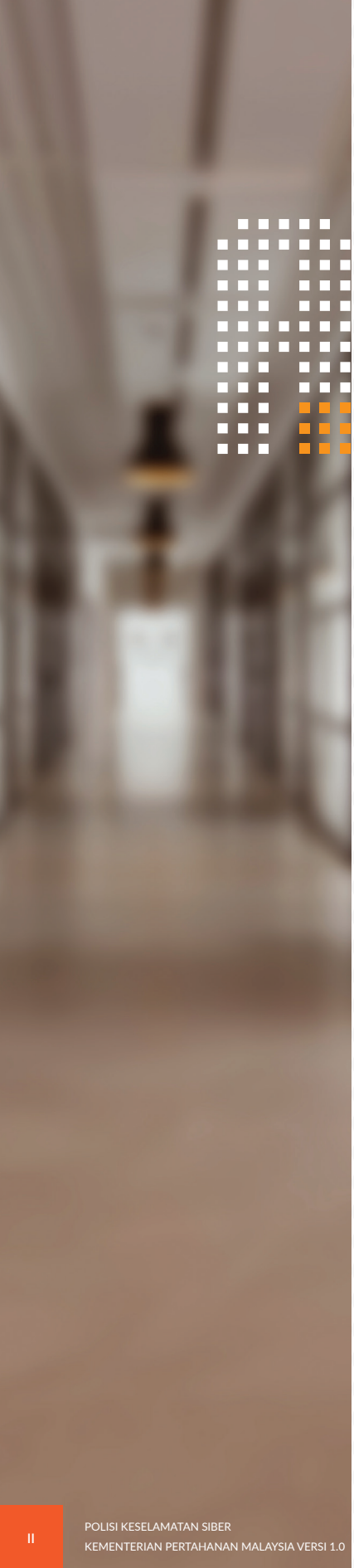
Cetakan Pertama 2022

Diterbitkan oleh:
Kementerian Pertahanan
Jalan Padang Tembak
50634 Kuala Lumpur
Portal: www.mod.gov.my

Dicetak Oleh
SUNSHOWER VENTURES SDN BHD
No. 187-1, Jalan LP 7/2, Kinrara Uptown,
43300 Seri Kembangan, Selangor.
Tel: +60123071166

KANDUNGAN

Perutusan ..... i-vii
Glosari / Terma Rujukan 1
Sejarah Dokumen 1
Tujuan 2
Latar Belakang 2
Objektif 2
Tadbir Urus 3
Aset ICT MINDEF 4
Risiko 6
Prinsip Keselamatan 7
Teknologi 8
Proses 10
Manusia 11
Pelan Pengurusan Keselamatan Maklumat 13
Pernyataan Polisi Keselamatan Siber MINDEF 14
Bidang A.1: Polisi Keselamatan Maklumat 18
(Information Security Policy)
Bidang A.2: Perancangan Bagi Keselamatan Organisasi 22
(Organization Of Information Security)
Bidang A.3: Keselamatan Sumber Manusia 36
(Human Resource Security)
Bidang A.4: Pengurusan Aset 42
(Asset Management)
Bidang A.5: Kawalan Akses 50
(Access Control)
Bidang A.6: Kriptografi 62
(Cryptography)
Bidang A.7: Keselamatan Fizikal Dan Persekitaran 66
(Physical And Environmental Security)
Bidang A.8: Keselamatan Operasi 78
(Operations Security)
Bidang A.9: Keselamatan Komunikasi 88
(Communications Security)
Bidang A.10: Pemerolehan, Pembangunan Dan Penyenggaraan Sistem 94
(System Acquisition, Development And Maintenance)
Bidang A.11: Hubungan Dengan Pembekal 104
(Supplier Relationship)
Bidang A.12: Pengurusan Insiden Keselamatan ICT 110
(ICT Security Incident Management)
Bidang A.13: Pengurusan Kesinambungan Perkhidmatan 116
(Business Continuity Management)
Bidang A.14: Pematuhan 122
(Compliance)
Lampiran A: Surat Akuan Pematuhan Polisi Keselamatan Siber Kementerian Pertahanan 127
Lampiran B: Rujukan 128



السلام عليكم ورحمة الله وبركاته

Alhamdulillah, syukur ke hadrat Allah, dengan limpah rahmat dan inayahnya, Polisi Keselamatan Siber Kementerian Pertahanan (PKS MINDEF) ini berjaya dihasilkan untuk rujukan seluruh warga Kementerian Pertahanan; warga Awam dan ATM.

PKS MINDEF merupakan dasar yang menggariskan kehendak, komitmen dan ekspektasi pengurusan tertinggi kementerian ini terhadap aspek keselamatan siber dan keselamatan maklumat. PKS MINDEF juga mengambil kira keperluan kementerian dari aspek keselamatan organisasi, perlindungan aset maklumat, perkhidmatan infrastruktur maklumat kritikal seperti pusat data dan rangkaian, data dan rekod digital terperingkat, elemen sumber manusia, dan penggunaan teknologi digital dalam memastikan kesinambungan perkhidmatan digital di Kementerian Pertahanan.

Justeru, penghasilan PKS MINDEF ini adalah sesuatu yang signifikan dan sejajar dengan tuntutan perkembangan teknologi digital serta landskap keselamatan maklumat di dalam persekitaran siber MINDEF.

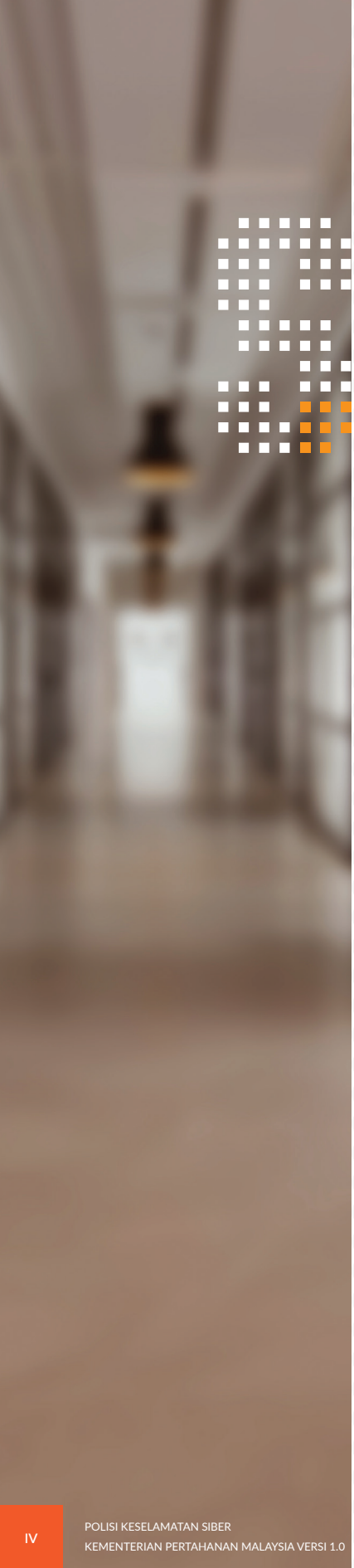
Setinggi-tinggi penghargaan dan terima kasih kepada Bahagian Pengurusan Maklumat yang bertindak sebagai *'focal point'* dan penyelaras dalam memastikan penglibatan wakil daripada pelbagai Bahagian, Jabatan dan Perkhidmatan ATM. Ini adalah untuk memastikan keterangkuman dan ketelusan dalam pembangunan dokumen ini dapat difahami dalam kalangan pemegang taruh utama kementerian.

Pematuhan kepada kandungan dan penguatkuasaan PKS MINDEF ini terpakai kepada semua warga Kementerian Pertahanan, tidak terkecuali pembekal, pakar perunding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF.

Dengan ini, saya menyeru agar semua Warga Kementerian Pertahanan, membaca, memahami, menghayati, mematuhi kandungan polisi ini serta mempraktikkannya dalam konteks kerja seharian.

Sekian, terima kasih.

YBHG. DATO' SRI MUEZ BIN ABD AZIZ
Ketua Setiausaha
Kementerian Pertahanan



السلام عليكم ورحمة الله وبركاته

Segala pujian dan syukur kepada Allah Subhanahu Wata'ala, di atas pelbagai kurniaan dan anugerah yang tidak terhitung buat kita semua. Selawat dan salam juga buat junjungan besar Nabi Muhammad Sallallahu Alaihi Wasallam, ahli keluarga, para sahabat serta pengikutpengikut baginda yang setia sehingga ke akhir zaman.

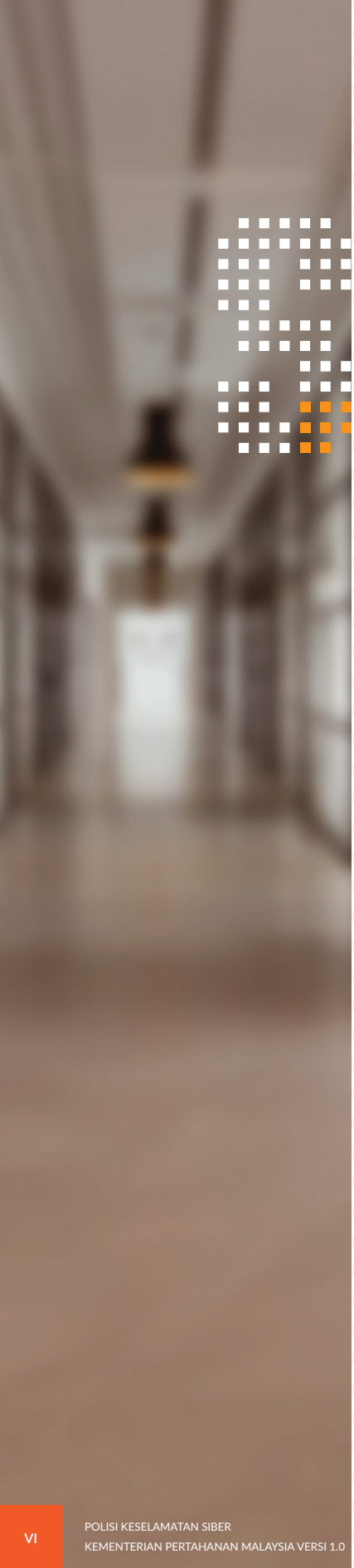
Alhamdulillah, kerana dengan limpahan rahmat dan izinNya, Bahagian Pengurusan Maklumat, Kementerian Pertahanan bersama-sama Angkatan Tentera Malaysia (ATM) telah berjaya menghasilkan Polisi Keselamatan Siber Kementerian Pertahanan Malaysia (PKS MINDEF) ini. Penggubalan PKS MINDEF ini adalah bagi menggantikan Dasar Keselamatan Teknologi Maklumat dan Komunikasi (DKICT) sedia ada dan seterusnya menjadi rujukan utama terhadap semua perkara berkaitan dasar dan polisi keselamatan siber serta pengurusan ICT yang terkini buat seluruh warga ATM termasuk warga awam MINDEF.

Ledakan kemajuan teknologi dewasa ini yang berkembang pesat seperti kemajuan *Industrial Revolution* (IR 4.0), I*nternet of Things* (IoT) dan *Big Data Analytics* telah mengubah dimensi pertahanan sesebuah negara. Oleh itu, dengan kewujudan PKS ini, saya optimis bahawa keupayaan ATM dan MinDef di dalam Domain Keselamatan Siber akan dapat terus diperkukuhkan sepertimana yang telah dihasratkan oleh Kertas Putih Pertahanan. Justeru, menjadi tanggungjawab kita semua sama ada sebagai pelaksana mahupun pengguna agar dapat meningkatkan kesedaran, kecekapan serta kompetensi diri demi memastikan aspek keselamatan ICT yang dimiliki sentiasa berada di tahap yang tertinggi sekaligus meminimumkan impak akibat insiden keselamatan siber ATM dan MinDef secara keseluruhannya.

Akhir kalam, saya ingin menyeru kepada semua peringkat warga ATM dan warga MinDef agar memahami, mematuhi serta menguatkuasakan PKS MINDEF ini. Laksanakanlah amanah ini dengan penuh ikhlas serta penuh rasa tanggungjawab bagi memastikan integriti pertahanan dan kedaulatan negara sentiasa terpelihara demi kebaikan kita semua bersama.

"KESELAMATAN NEGARA,
TANGGUNGJAWAB BERSAMA"

TAN SRI DATO' SRI HJ. AFFENDI BIN BUANG
Jeneral TUDM
Panglima Angkatan Tentera



السلام عليكم ورحمة الله وبركاته

Syukur ke hadrat Ilahi dan setinggi penghargaan saya rakamkan kepada semua yang terlibat dalam pembangunan Polisi Keselamatan Siber Kementerian Pertahanan (PKS MINDEF) ini. Sebagai organisasi di bawah sektor Keselamatan dan Pertahanan dalam CNII *(Critical National Information Infrastructure)*, PKS MINDEF memainkan peranan yang besar dalam mencorakkan tadbir urus, komitmen pengurusan tertinggi serta menggariskan asas-asas keselamatan maklumat dan keselamatan siber yang perlu dilaksanakan dan dipatuhi oleh semua warga Kementerian Pertahanan.

Penggubalan, pelaksanaan, penguatkuasaan dan juga pematuhan kepada polisi ini merupakan kaedah kawalan pentadbiran yang menggunapakai prinsip *Defense-in-Depth* bagi memastikan objektif keselamatan dan elemen Segitiga Keselamatan Maklumat iaitu *Confidentiality*, *Integrity* dan *Availability* terpelihara sekaligus meminimumkan risiko kepada keselamatan maklumat dan ruang siber di Kementerian Pertahanan, jabatan dan agensi serta seluruh Perkhidmatan ATM.

Dokumen PKS MINDEF menggantikan Dasar Keselamatan ICT (DKICT MINDEF) versi 5.0 dan diperakukan menerusi kelulusan Jawatankuasa Pemandu ICT MINDEF. Penggantian ini wajar jika mengambil kira landskap semasa yang menyaksikan peningkatan cabaran global seperti ancaman bukan tradisional, peperangan asimetri, *non-state actor*, aktiviti espionaj dan *hacktivism*, selain keperluan-keperluan baharu yang telah dikenalpasti dalam Kertas Putih Pertahanan.

Dengan berlandaskan kaedah pengurusan risiko dan juga piawaian ISO/IEC 27001 Sistem Pengurusan Keselamatan Maklumat, PKS MINDEF membolehkan pengurusan keselamatan maklumat dan siber diselaraskan bagi menjamin kesinambungan keselamatan perkhidmatan digital yang menggunakan *Information & Communication Technology* (ICT) dan *Operational Technology* (OT) di kementerian dan juga ATM. Setiap aset digital yang menyokong fungsi kritikal pertahanan adalah merupakan sasaran penting yang perlu dilindungi dan dipertahankan ketersediaannya.

Pelancaran PKS MINDEF ini adalah seiring dengan garis masa inisiatif transformasi digital sektor awam dan juga program-program Pendigitalan Perkhidmatan yang sedang dilaksanakan dalam Pelan Strategik Pendigitalan MINDEF (PSP MINDEF) 2021-2025. Justeru, saya berharap polisi ini dapat dihayati dan dipatuhi oleh semua warga kementerian agar visi untuk mempertahankan Malaysia sebagai sebuah negara yang selamat, berdaulat dan makmur dapat dicapai.

Sekian, wassalamualaikum warahmatullahi wabarakatuh.

YBRS. DR. ANIS BIN MAHMUD @ ABDUL SAMAD
Timbalan Ketua Setiausaha (Pengurusan)
merangkap Ketua Pegawai Maklumat dan Ketua Pegawai Digital
Kementerian Pertahanan

GLOSARI / TERMA RUJUKAN

ATM

Angkatan Tentera Malaysia

BKP

Bahagian Khidmat Pengurusan, Kementerian Pertahanan

BPM

Bahagian Pengurusan Maklumat

BSEP

Bahagian Siber dan Elektromagnetik Pertahanan

CERT

Computer Emergency Response Team

CERT Perkhidmatan Tentera dan Awam

Organisasi CERT di peringkat Perkhidmatan Tentera dan Awam

CDO

Ketua Pegawai Digital *(Chief Digital Officer)*

CIO

Ketua Pegawai Maklumat *(Chief Information Officer)*

CISO

Ketua Pegawai Keselamatan Maklumat *(Chief Information Security Officer)*

CGSO

Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia *(Chief Government Security Office)*

CNII

Infrastruktur Maklumat Kritikal Negara

ICTSO

Pegawai Keselamatan ICT *(ICT Security Officer)*

JPICT

Jawatankuasa Pemandu ICT MINDEF

Kriptografi

Kriptografi adalah mekanisme penyulitan data menggunakan kaedah algoritma matematik. Transformasi penyulitan data terbahagi kepada dua iaitu kaedah penyulitan *(encryption)* dan penyahsulitan *(decryption)*. Teknik ini digunapakai dalam keselamatan maklumat dan data bagi menjaga kerahsiaan dan integriti sesuatu maklumat.

Malware

Perisian hasad seperti *virus*, *worm*, *bot*, *spyware*, *adware*

MINDEF

MINDEF ditakrifkan sebagai warga awam dan Perkhidmatan ATM yang berkhidmat dalam Kementerian Pertahanan, termasuk di Bahagian, Jabatan, Markas dan premis ATM.

MINDEFCERT

Pasukan CERT MINDEF

NACSA

National Cyber Security Agency

NC4

National Cyber Coordination and Control Center

Pengurus ICT

Ketua Jabatan ICT yang bertanggungjawab dalam memantau personel dan menjadi tonggak utama kepada program-program keselamatan dibawah Jabatan tersebut.

Perkhidmatan digital

Perkhidmatan digital adalah perkhidmatan ICT yang disediakan oleh MINDEF dan ATM, termasuklah perkhidmatan yang dibangunkan secara dalaman, penyumberluaran, atau menerusi *Managed Information Services* atau perkhidmatan pengkomputeran awan (*Cloud Services*: IAAS,SAAS, PAAS) dan setara dengannya.

SEJARAH DOKUMEN

TARIKH KUATKUASA	PEMAKLUMAN	KELULUSAN	VERSI
22 Februari 2022	Memo Edaran Penguatkuasaan Polisi Keselamatan Siber Kementerian Pertahanan Malaysia	Mesyuarat Jawatankuasa Pemandu ICT MINDEF Bil 1/2022	1.0

TUJUAN

Polisi Keselamatan Siber (PKS), Kementerian Pertahanan Malaysia (MINDEF) ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital ICT MINDEF dalam melindungi maklumat di ruang siber.

LATAR BELAKANG

Polisi ini dibangunkan untuk menjamin kesinambungan perkhidmatan MINDEF dengan meminimumkan kesan insiden keselamatan siber. Polisi ini akan memudahkan perkongsian maklumat sesuai dengan keperluan operasi MINDEF bagi memastikan semua maklumat dilindungi.

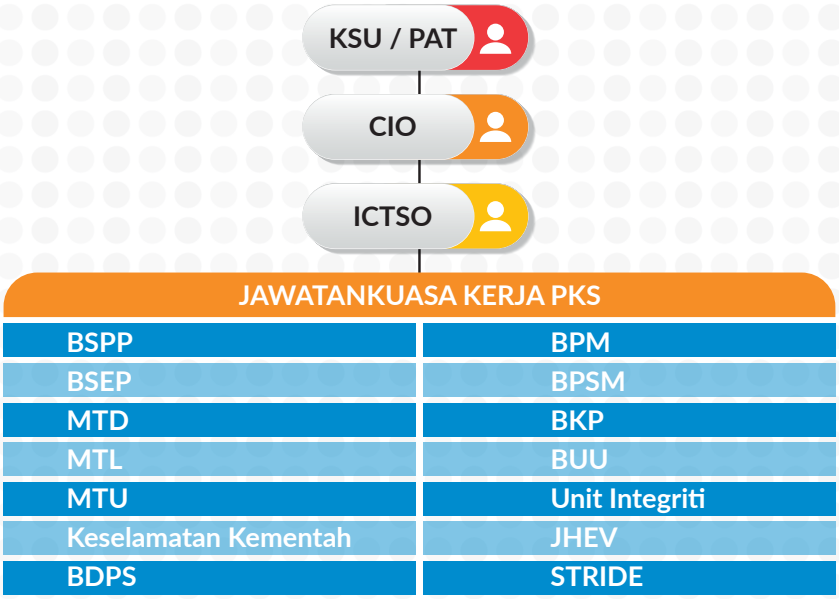
OBJEKTIF

Objektif utama Polisi Keselamatan Siber ini dibangunkan adalah seperti yang berikut:

- Menerangkan kepada semua pengguna merangkumi warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber;
- Memastikan keselamatan penyampaian perkhidmatan MINDEF di tahap tertinggi sekali gus meningkatkan tahap keyakinan pihak-pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;
- Memastikan kelancaran operasi MINDEF dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;
- Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan yang berlaku dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan
- Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

TADBIR URUS

Bagi memastikan keberkesanan dan kejayaan pelaksanaan PKS MINDEF, satu tadbir urus telah diwujudkan seperti berikut :



Rajah 1: Struktur Tadbir Urus Polisi Keselamatan Siber

Keahlian Jawatankuasa ini adalah seperti berikut :

Penaung :	Ketua Setiausaha (KSU) / Panglima Angkatan Tentera (PAT)
Pengerusi :	Ketua Pegawai Maklumat (CIO)
Timbalan Pengerusi :	ICTSO
Urusetia :	Tim Keselamatan (Bahagian Pengurusan Maklumat)

Ahli- ahli Jawatankuasa Kerja Polisi Keselamatan Siber yang terdiri daripada :

- Bahagian Staf Perisikan Pertahanan (BSPP)
- Bahagian Siber dan Elektromagnetik Pertahanan (BSEP)
- Markas Tentera Darat (MTD)
- Markas Tentera Laut (MTL)
- Markas Tentera Udara (MTU)
- Keselamatan Kementah
- Bahagian Dasar dan Perancangan Strategik (BDPS)
- Bahagian Pengurusan Maklumat (BPM)
- Bahagian Pengurusan Sumber Manusia (BPSM)
- Bahagian Khidmat Pengurusan (BKP)
- Bahagian Undang-Undang (BUU)
- Unit Integriti (UI)
- Jabatan Hal Ehwal Veteran (JHEV)
- Institut Penyelidikan Sains dan Teknologi Pertahanan (STRIDE)

ASET ICT MINDEF

Aset ICT MINDEF merangkumi Maklumat, Aliran Data, Platform Aplikasi dan Perisian, Peranti Fizikal dan Sistem, Sistem Luaran serta Sumber Luaran seperti berikut:

i) Maklumat

Semua penyedia perkhidmatan dalam MINDEF hendaklah mengenal pasti maklumat yang dijana dan hendaklah mengasingkannya mengikut kategori:

a) Maklumat Rahsia Rasmi

Di bawah Akta Rahsia Rasmi 1972 (Akta 88), maksud Maklumat Rahsia Rasmi ialah apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 (Akta 88) dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai "Rahsia Besar", "Rahsia", "Sulit" atau "Terhad" mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 28 Akta Rahsia Rasmi 1972.

b) Maklumat Rasmi

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

c) Maklumat Pengenalan Peribadi

Maklumat Pengenalan Peribadi (PII atau *Personally Identifiable Information*) ialah maklumat yang boleh digunakan secara tersendiri atau digunakan bersama maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu. PII boleh juga terkandung dalam Maklumat Rahsia Rasmi.

d) Data Terbuka

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

ii) Aliran Data

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

a) Saluran komunikasi dan aliran data antara sistem di MINDEF;
b) Saluran komunikasi dan aliran data ke sistem luar; dan
c) Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.

iii) **Platform Aplikasi dan Perisian**

Semua platform aplikasi dan perisian hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

iv) **Peranti Fizikal dan Sistem**

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

a) Pelayan;
b) Peranti/Peralatan Rangkaian;
c) Workstation, Komputer Desktop/Komputer Riba;
d) Telefon/peranti pintar;
e) Media Storan;
f) Peranti dengan sambungan ke rangkaian, contohnya pengimbas, mesin pencetak, sistem kawalan akses, alat kawalan dan sistem kamera litar tertutup (CCTV);
g) Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi Kerajaan; dan
h) Peranti pengesahan *(authentication devices)*, contohnya token keselamatan, dongle dan alat pengimbas biometrik.

v) **Sistem Luaran**

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

vi) **Sumber Luaran**

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

a) Perisian Sebagai Satu Perkhidmatan (Saas);
b) Platform Sebagai Satu Perkhidmatan (PaaS);
c) Infrastruktur Sebagai Satu Perkhidmatan (IaaS);
d) Storan Pengkomputeran Awan *(Cloud Storage)*; dan
e) Pemantauan Keselamatan.

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

RISIKO

i) MINDEF hendaklah mengenal pasti risiko yang berkaitan dengan maklumat yang terlibat. Risiko ialah kebarangkalian sesuatu kecelakaan atau bencana berlaku yang menyebabkan kerosakan sehingga terjejas fungsi perkhidmatan sesuatu jabatan. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam ruang siber MINDEF.

ii) Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran siber MINDEF.

iii) Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

a) Kerentanan *(Vulnerability)*

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

b) Ancaman *(Threat)*

MINDEF hendaklah mengenal pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

c) Impak *(Impact)*

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

d) Tahap Risiko

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

e) Penguraian Risiko

- Penguraian risiko hendaklah dikenal pasti untuk menentukan sama ada risiko perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/faedahnya.
- Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala dengan mengambil kira perkara berikut:
  - Teknologi

    Teknologi hendaklah dikenal pasti untuk mengurangkan risiko. Sebagai contoh, *firewall* digunakan untuk menghadkan capaian logikal kepada sistem tertentu.

- Proses

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

- Manusia

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

f) Pengurusan Risiko

- Penyedia perkhidmatan digital di MINDEF hendaklah memastikan tadbir urus pengurusan risiko diwujudkan dengan mengambil kira perkara berikut:

  - mengenal pasti kerentanan;
  - mengenal pasti ancaman;
  - menilai risiko;
  - menentukan penguraian risiko;
  - memantau keberkesanan penguraian risiko; dan
  - memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

- Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya sekali setahun oleh Bahagian/Jabatan masing-masing dan dimaklumkan kepada Ketua Jabatan atau Jawatankuasa yang ditentukan oleh Ketua Jabatan.

PRINSIP KESELAMATAN

i) Prinsip keselamatan hendaklah dipilih berdasarkan penilaian risiko dan kategori maklumat yang dikendalikan oleh sistem. Bagi mencapai objektif keselamatan maklumat, MINDEF hendaklah melaksanakan prinsip keselamatan seperti yang berikut:

a) Prinsip "Perlu-Tahu" *(Need-to-know)*

MINDEF hendaklah melaksanakan mekanisme bagi memberikan kebenaran kepada capaian maklumat. Maklumat yang dicapai oleh pengguna yang dibenarkan hendaklah berdasarkan prinsip "Perlu-Tahu" yang membenarkan capaian maklumat yang diperlukan untuk melaksanakan tugasnya sahaja.

Bagi capaian spesifik Maklumat Rahsia Rasmi, penggunaan yang dibenarkan hendaklah dihadkan kepada masa, lokasi, peranan dan fungsi pengguna tersebut.

b) Hak Keistimewaan Minimum *(Minimum privilege)*

Pengguna hendaklah diberikan hak keistimewaan minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Prinsip ini digunakan untuk menyekat hak akses kepada aplikasi, sistem, proses dan peranti kepada pengguna yang dibenarkan untuk melaksanakan aktiviti. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

c) Pengasingan Tugas *(Segregation of duty)*

Bagi mengekalkan prinsip semak-dan-imbang *(check and balance)*, MINDEF hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

d) Kawalan Capaian Berdasarkan Peranan *(Role based access control)*

Capaian sistem hendaklah dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu adalah berdasarkan peranan tersebut.

e) Peminimuman Data

Menghadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.

TEKNOLOGI

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

(a) Peringkat Pemprosesan Data

(1) Data-dalam-simpanan *(Data-at-rest)*

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

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

(2) Data-dalam-pergerakan *(Data-in-motion)*

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

(3) Data-dalam-penggunaan *(Data-in-use)*

- MINDEF hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-penggunaan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Di samping itu, teknologi untuk menentukan asal data dan tanpa sangkalan mungkin diperlukan. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data dalam penggunaan.

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

(4) Perlindungan Ketirisan Data *(Data Leakage Protection)*

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

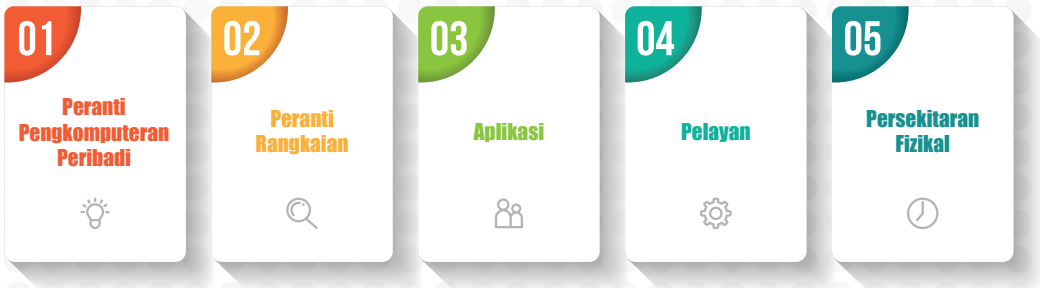
- Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

(b) Elemen Dalam Persekitaran Pengkomputeran

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

Maklumat Rahsia Rasmi hendaklah disimpan dan diproses dalam persekitaran pengkomputeran mengikut Arahan Keselamatan yang dikeluarkan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) atau mendapat pengesahan daripada CGSO.

Setiap projek ICT yang dibangunkan di MINDEF hendaklah mempunyai Pelan Pengurusan Keselamatan Maklumat tersendiri yang mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:



PROSES

1. Warga MINDEF hendaklah melindungi keselamatan siber dengan melaksanakan perkara-perkara berikut:

(i) Konfigurasi Asas

(a) Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi prasyarat pentauliahan sistem.

(b) Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan.

(ii) Kawalan Perubahan Konfigurasi

(a) Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.

(b) Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asas terkini.

(c) Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan.

(iii) Sandaran

(a) Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang sedang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan.

(b) Media sandaran hendaklah disimpan dalam persekitaran yang selamat dan di lokasi yang berasingan.

(iv) Kitaran Pengurusan Aset

(a) Pindah

(1) Pemindahan hak milik aset berlaku dalam keadaan berikut:

(i) Warga MINDEF meninggalkan agensi disebabkan oleh persaraan, perletakkan jawatan atau penugasan semula;
(ii) Aset yang dikongsi untuk kegunaan sementara;
(iii) Pemberian aset kepada agensi lain; dan
(iv) Aset dikembalikan setelah tamat tempoh sewaan

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

(b) Pelupusan

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

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

(3) Pelupusan boleh dalam bentuk pemusnahan fizikal dan/atau sanitasi data.

(4) Sanitasi data hendaklah mengikut garis panduan yang sedang berkuat kuasa.

(c) Kitaran Hayat

(1) Kitaran hayat data hendaklah diuruskan Akta Arkib Negara 2003 (Akta 629).

(2) Akta Arkib Negara 2003 (Akta 629) memberikan mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umum selama lima tahun.

MANUSIA

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

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

(i) Kompetensi Pengguna

(a) Kompetensi pengguna termasuk:

(1) Kesedaran amalan terbaik keselamatan maklumat dengan memupuk amalan baik keselamatan siber dengan mewujudkan komunikasi ICT dan program kesedaran keselamatan siber.

(2) Kemahiran menggunakan alat keselamatan dengan menyediakan latihan yang mencukupi kepada warga MINDEF berhubung alat-alat keselamatan berkaitan untuk memastikan mereka mampu untuk melaksanakan tugas harian mereka.

(b) Setiap orang yang diberi kuasa untuk mengendalikan dokumen terperingkat, kompetensi tambahan pengguna selaras dengan arahan/pekeliling semasa adalah diharapkan.

(ii) Kompetensi Pelaksana

(a) Warga MINDEF yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.

(b) Pegawai Keselamatan ICT hendaklah memenuhi syarat-syarat berikut:

(1) Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber.
(2) Memenuhi keperluan pembelajaran berterusan.
(3) Menimba pengalaman yang mencukupi dalam bidang keselamatan siber.
(4) Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa.

(c) Pegawai Keselamatan ICT yang dilantik oleh MINDEF hendaklah memenuhi keperluan kompetensi di atas. Pegawai Keselamatan ICT bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan di MINDEF.

(iii) Peranan

(a) Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna.
(b) Setiap orang yang terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani *Non-disclosure Agreement (NDA)* seperti Arahan Keselamatan. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan.
(c) Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka.
(d) Warga MINDEF yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT Jabatan dikembalikan sekiranya berlaku perubahan peranan.
(e) Warga MINDEF yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan yang berkaitan seperti tersenarai dalam senarai aset Nota Serah Tugas.
(f) Warga MINDEF lain yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan dengan diselia oleh kakitangan yang dipertanggungjawabkan oleh Jabatan.

PELAN PENGURUSAN KESELAMATAN MAKLUMAT

1. Setiap projek yang berimpak tinggi di MINDEF hendaklah menyediakan Pelan Pengurusan Keselamatan Maklumat. Pelan ini mengandungi maklumat terperinci yang menyatakan keutamaan aplikasi, kawalan capaian dan keperluan-keperluan khusus yang lain.

2. Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), Polisi Keselamatan Siber Kementerian Pertahanan Malaysia (PKS MINDEF) dan surat pekeliling/arahan terkini untuk menangani isu-isu operasi projek.

3. Pelan ini hendaklah mengenal pasti perlindungan data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data.

4. Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

   (i) Peranti Pengkomputeran Peribadi

   (a) Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, *workstation*, telefon pintar, tablet dan peranti storan.

   (b) Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada Ketua Jabatan. Walau bagaimanapun, peranti pengkomputeran peribadi milik persendirian hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk ke kawasan larangan. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

   (ii) Peranti Rangkaian

   (a) Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti *switch*, *router*, *firewall*, peranti *Virtual Private Network* (VPN) dan kabel.

   (b) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

   (iii) Aplikasi

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

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

(iv) Pelayan

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

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

(v) Persekitaran Fizikal

(a) Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.

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

(c) Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip *defence-in-depth*.

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

PERNYATAAN POLISI KESELAMATAN SIBER MINDEF

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

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

(i) Kerahsiaan

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

(ii) Integriti

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

(iii) **Tidak Boleh Disangkal**

Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal.

(iv) **Kesahihan**

Data dan maklumat hendaklah dipastikan kesahihannya.

(v) **Ketersediaan**

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

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

3. 14 bidang keselamatan yang terlibat di dalam Polisi Keselamatan Siber MINDEF diterangkan dengan lebih jelas dan teratur seperti berikut:

BIDANG A.1

A.1.1 Hala Tuju Pengurusan Untuk Keselamatan Maklumat 18
(Management Directions for Information Security)
A.1.1.1 Polisi Keselamatan Maklumat *(Policies for Information Security)*
A.1.1.2 Kajian Semula Polisi untuk Keselamatan Maklumat
(Review of Policies for Information Security)

Polisi Keselamatan Maklumat

Information Security Policy

A.1.1 HALA TUJU PENGURUSAN UNTUK KESELAMATAN MAKLUMAT

(MANAGEMENT DIRECTIONS FOR INFORMATION SECURITY)

Objektif: Untuk menjelaskan keperluan penggubalan dan pelaksanaan dasar-dasar berkaitan keselamatan maklumat dan keselamatan siber yang dinamakan Polisi Keselamatan Siber (PKS) Kementerian Pertahanan Malaysia. Penggubalan PKS menggariskan halatuju dan sokongan pihak pengurusan tertinggi dalam memastikan objektif polisi ini dapat dicapai selaras dengan tanggungjawab MINDEF sebagai peneraju perlindungan organisasi Infrastruktur Maklumat Kritikal Negara (CNII) bagi sektor pertahanan.

Kawalan:	Perkara:
A.1.1.1	**Polisi Keselamatan Maklumat** *(Policies for Information Security)*

Penggubalan dan pelaksanaan polisi ini adalah di bawah tanggungjawab bersama Ketua Setiausaha (KSU) dan Panglima Angkatan Tentera (PAT).

Polisi ini dimuktamadkan menerusi kelulusan Jawatankuasa Pemandu ICT (JPICT) MINDEF.

Jawatankuasa pembangunan polisi dan kajian semula polisi adalah diketuai oleh Ketua Pegawai Maklumat (CIO) dan Ketua Pegawai Keselamatan Maklumat (CISO), dengan dibantu Pegawai Keselamatan ICT (ICTSO) dan ahli jawatankuasa yang dilantik.

Polisi Keselamatan Siber MINDEF mestilah dipatuhi oleh warga, pembekal, pakar runding dan pihak yang mengakses dan menggunakan perkhidmatan digital MINDEF.

Polisi ini hendaklah digubal, dilulus, diterbit dan dimaklumkan oleh pihak pengurusan MINDEF kepada warga, pembekal, pakar runding dan pihak yang mengakses dan menggunakan perkhidmatan digital MINDEF.

Peranan:	KSU / PAT / JPICT / CIO / CISO / ICTSO

Kawalan:	Perkara:
A.1.1.2	**Kajian Semula Polisi untuk Keselamatan Maklumat** *(Review of Policies for Information)*

Polisi ini adalah tertakluk kepada semakan dan pindaan sebagai penambahbaikan berterusan selaras dengan perubahan hala tuju strategik, perubahan dasar dan perundangan kerajaan, keperluan perkhidmatan, perekayasaan proses, perubahan arkitektur data, aplikasi dan teknologi, kepentingan ekonomi dan sosial, ancaman risiko keselamatan siber semasa, serta sebarang justifikasi yang relevan dengan peranan MINDEF.

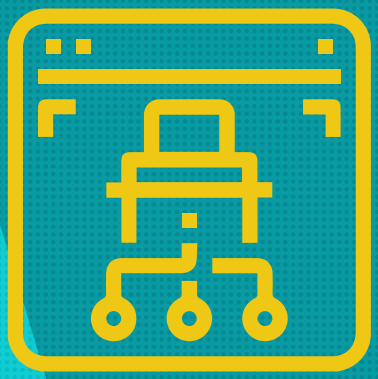
Prosedur yang berkaitan dengan kajian semula Polisi Keselamatan Siber MINDEF adalah seperti berikut:

Peranan:	JPICT / CIO / CISO / ICTSO

BIDANG A.2

A.2.1 Perancangan Dalaman *(Internal Organization)* 23
A.2.1.1 Peranan dan Tanggungjawab Keselamatan Maklumat *(The Role and Responsibility of Information Security)*
A.2.1.2 Pengasingan Tugas *(Segregation of Duties)*
A.2.1.3 Hubungan Dengan Pihak Berkuasa *(Contact with Authorities)*
A.2.1.4 Hubungan Dengan Kumpulan Berkepentingan Yang Khusus *(Contact with Special Interest Groups)*
A.2.1.5 Keselamatan Maklumat dalam Pengurusan Projek *(Information Security in Project Management)*

A.2.2 Peranti Mudah Alih dan Telekerja *(Mobile Devices and Teleworking)* 33
A.2.2.1 Polisi Peranti Mudah Alih *(Mobile Device Policy)*
A.2.2.2 Telekerja *(Teleworking)*



Perancangan Bagi Keselamatan Organisasi

Organization of Information Security

A.2.1 PERANCANGAN DALAMAN *(INTERNAL ORGANIZATION)*

Objektif: Menerangkan peranan dan tanggungjawab semua pihak yang terlibat dengan lebih jelas dan teratur untuk mencapai objektif Polisi Keselamatan Siber MINDEF.

Kawalan:	Perkara:
A.2.1.1	**Peranan dan Tanggungjawab Keselamatan Maklumat** *(The Role and Responsibility of Information Security)*

(i) **Ketua Setiausaha**

Peranan dan tanggungjawab adalah seperti yang berikut:

(a) Memastikan penguatkuasaan pelaksanaan Polisi ini;
(b) Memastikan warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini;
(c) Memastikan semua keperluan MINDEF seperti sumber kewangan, sumber manusia dan perlindungan keselamatan adalah mencukupi;
(d) Memastikan pengurusan risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam Polisi ini;
(e) Mempengerusikan Mesyuarat JPICT MINDEF; dan
(f) Melantik CIO dan ICTSO.

Peranan:	Ketua Setiausaha (KSU)

ii) **Panglima Angkatan Tentera**

Peranan dan tanggungjawab adalah seperti yang berikut:

(a) Memastikan pelaksanaan organisasi keselamatan ICT ATM berfungsi dengan berkesan;
(b) Memastikan semua pengguna memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini;
(c) Memastikan semua keperluan MINDEF seperti sumber kewangan, sumber manusia dan perlindungan keselamatan adalah mencukupi; dan
(d) Memastikan pengurusan risiko, sumber manusia dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam Polisi ini.

Peranan:	Panglima Angkatan Tentera (PAT)

Kawalan:	Perkara:
A.2.1.1	**Peranan dan Tanggungjawab Keselamatan Maklumat** *(The Role and Responsibility of Information Security)*

(iii) Ketua Pegawai Maklumat (CIO)

CIO adalah pegawai yang dilantik oleh Ketua Jabatan mengikut Surat Arahan Ketua Setiausaha Negara Penamaan Ketua Pegawai Maklumat Sektor Awam Tahun 2000 dan Pekeliling Perkhidmatan Bilangan 5 Tahun 2007.

Peranan dan tanggungjawab CIO adalah seperti yang berikut:

(a) Membantu KSU / Ketua Jabatan dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber seperti yang ditetapkan di dalam Polisi ini;
(b) Memastikan kawalan keselamatan maklumat dalam MINDEF diseragam dan diselaraskan dengan sebaiknya;
(c) Memastikan Pelan Strategik Pendigitalan MINDEF mengandungi aspek keselamatan siber;
(d) Menyelaras pelan latihan dan program kesedaran keselamatan siber; dan
(e) Mempengerusikan Mesyuarat JPICT MINDEF dengan penurunan kuasa oleh KSU.

Peranan:	CIO

(iv) **Ketua Pegawai Keselamatan Maklumat (CISO)**

Peranan dan tanggungjawab CISO yang dilantik adalah seperti yang berikut:

(a) Menggariskan direktif strategik keselamatan maklumat serta menghasilkan polisi dan menubuhkan peranan dan fungsi keselamatan maklumat organisasi di bawah Kementerian Pertahanan bagi melaksanakan Pelan Pengurusan Krisis Siber Negara dan Prosedur Tindak Balas, Komunikasi dan Penyelarasan Pengurusan Krisis Siber Negara

(b) Meneraju dan memantau pelaksanaan perkara-perkara berkaitan pengurusan keselamatan siber ATM dan MINDEF melalui Mesyuarat Jawatankuasa Induk Keselamatan Siber.

(c) Memastikan agensi dan/atau organisasi ATM dan MINDEF melaksanakan ISMS atau yang setara dengannya bagi mengurangkan risiko insiden keselamatan siber.

(d) Memastikan agensi dan/atau organisasi ATM dan MINDEF membangunkan dan melaksanakan prosedur tindak balas insiden keselamatan siber serta pelan kesinambungan perkhidmatan dengan mengetuai MINDEFCERT.

(e) Memastikan agensi dan/atau organisasi ATM dan MINDEF melaksanakan program-program kesiapsiagaan keselamatan siber.

(f) Membuat analisis, mengeluarkan amaran dan menyediakan laporan situasi ancaman siber bagi sektor pertahanan serta cadangan-cadangan mitigasi kepada MKN.

(g) Memastikan serta memantau tindakan-tindakan yang diambil oleh agensi dan/atau organisasi ATM dan MINDEF semasa krisis.

(h) Melaksanakan pengauditan, kajian semula dan merumuskan laporan ancaman keselamatan siber bagi sektor pertahanan kepada MKN; dan

(i) Bekerjasama dengan agensi-agensi berkaitan dalam menangani ancaman atau insiden keselamatan siber serta memperakukan langkah-langkah baik pulih dengan segera.

Peranan:	CISO

(v) **Pegawai Keselamatan ICT (ICTSO)**

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti yang berikut:

(a) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini;
(b) Merangka pengurusan risiko dan audit keselamatan siber berpandukan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat yang berkuat kuasa;
(c) Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlakunya ancaman keselamatan siber dan memberikan khidmat nasihat, tatacara pelaporan serta menyediakan langkah-langkah perlindungan yang bersesuaian;
(d) Melaporkan insiden keselamatan siber kepada NACSA / NC4 dan seterusnya membantu dalam penyiasatan atau pemulihan;
(e) Melaporkan insiden keselamatan siber kepada CIO bagi insiden yang memerlukan Pengurusan Kesinambungan Perkhidmatan (PKP);
(f) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera;
(g) Melaksanakan pematuhan Polisi ini oleh warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF;
(h) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber;
(i) Menyedia dan merangka latihan dan program kesedaran keselamatan siber; dan
(j) Mempengerusikan Mesyuarat Kajian Semula Pengurusan ISMS (ISO/IEC 27001:2013).

Peranan:	ICTSO

(vi) **Pengurus ICT**

Pengurus ICT adalah pegawai yang mengetuai bahagian ICT Jabatan dan Perkhidmatan ATM. Peranan dan tanggungjawab Pengurus ICT ialah melaksanakan keperluan Polisi ini dalam operasi semasa seperti yang berikut:

(a) Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu;
(b) Pembelian atau peningkatan perisian dan sistem komputer;
(c) Perolehan teknologi dan perkhidmatan komunikasi baharu;
(d) Menentukan pembekal dan rakan usaha sama menjalani tapisan keselamatan;
(e) Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat kerajaan yang berkuat kuasa;dan
(f) Memastikan setiap sistem yang dibangunkan telah dibuat ujian keselamatan.

Peranan:	Pengurus ICT

(vii) **Pentadbir Sistem ICT**

Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti yang berikut:

(a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;
(b) Menentukan ketepatan dan kesahihan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi ini;
(c) Memantau aktiviti capaian sistem aplikasi;
(d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta;
(e) Menganalisis dan menyimpan rekod jejak audit;
(f) Menyediakan laporan mengenai aktiviti capaian secara berkala; dan
(g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada personel di dalam keadaan yang baik.

Peranan:	Pentadbir Sistem ICT

(viii) Jawatankuasa Pemandu ICT (JPICT)

JPICT MINDEF adalah jawatankuasa yang bertanggungjawab untuk menilai dan meluluskan keperluan dan keselamatan ICT Jabatan / Bahagian / Perkhidmatan ATM. JPICT MINDEF dipengerusikan oleh KSU / TKSU dengan keahlian terdiri daripada Ketua Jabatan / Bahagian / Perkhidmatan ATM yang dilantik dan diurus setia oleh BPM.

Peranan dan tanggungjawab JPICT seperti yang terkandung dalam Surat Pekeliling Am Bil 3 Tahun 2015 ialah merancang dan menentukan langkah-langkah keselamatan siber.

Peranan:	JPICT MINDEF

(ix) **Jawatankuasa Teknikal ICT (JTICT) MINDEF**

JTICT MINDEF adalah jawatankuasa yang bertanggungjawab untuk menilai dan menyokong aspek teknikal bagi keperluan dan keselamatan ICT Bahagian / Jabatan / Perkhidmatan ATM.

JTICT MINDEF 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.

Peranan dan tanggungjawab JTICT seperti yang terkandung dalam Surat Pekeliling Am Bil 3 Tahun 2015 ialah merancang dan menentukan langkahlangkah keselamatan siber.

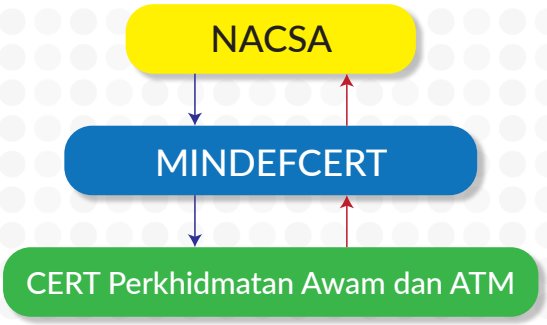
Peranan:	JTICT MINDEF

(x) *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 / Perkhidmatan. Urus setia bagi MINDEFCERT ialah BPM dan BSEP.

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 Agensi Keselamatan Siber Negara (NASCA) seperti di Rajah 2;
(e) Menasihatkan Jabatan / Bahagian / Perkhidmatan supaya mengambil tindakan pemulihan dan pengukuhan;
(f) Memaklumkan sebarang ancaman dan insiden keselamatan ICT kepada Jabatan / Bahagian / Perkhidmatan ; dan
(g) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baharu dapat dielakkan.



Rajah 2 : Carta Pelaporan Insiden Keselamatan ICT MINDEF

Peranan:	MINDEFCERT

(xi) **Pengguna**

Peranan dan tanggungjawab pengguna adalah seperti yang berikut:

(a) Membaca, memahami dan mematuhi Polisi ini;
(b) Mengetahui dan memahami implikasi kepada persekitaran keselamatan siber daripada tindakannya;
(c) Menjalani tapisan keselamatan sekiranya diperlukan dikehendaki berurusan dengan maklumat rasmi terperingkat;
(d) Mematuhi prinsip-prinsip keselamatan Polisi ini dan menjaga kerahsiaan maklumat Kerajaan;
(e) Melaksanakan langkah - langkah perlindungan seperti yang berikut:

1) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
2) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
3) Menentukan maklumat sedia untuk digunakan;
4) Menjaga kerahsiaan maklumat;
5) Mematuhi dasar, piawaian dan garis panduan keselamatan siber yang ditetapkan;
6) Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
7) Menjaga kerahsiaan kawalan keselamatan siber dari diketahui umum.

(f) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada MINDEFCERT dengan segera;
(g) Menghadiri program-program kesedaran mengenai keselamatan siber; dan
(h) Bersetuju dengan terma dan syarat yang terkandung di dalam Polisi ini dan menandatangani **Surat Akuan Pematuhan Polisi Keselamatan Siber Kementerian Pertahanan Malaysia (LAMPIRAN A)**.

Peranan:	Pengguna

Kawalan:	Perkara:
A.2.1.2	**Pengasingan Tugas** *(Segregation of Duties)*

Seseorang yang dilantik perlu mempunyai pengetahuan atau pengalaman dalam bidang ICT.

Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;
(ii) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi;
(iii) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan di dalam *production environment*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan
(iv) Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

Peranan:	Pengurus ICT

Kawalan:	Perkara:
A.2.1.3	**Hubungan Dengan Pihak Berkuasa** *(Contact with Authorities)*

Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab MINDEF;
(ii) Mewujud dan mengemas kini prosedur / senarai pihak berkuasa perundangan / pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah **Polis Diraja Malaysia dan Suruhanjaya Komunikasi Dan Multimedia**. Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta Bomba; dan
(iii) Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden dan tidak berkompromi kepada sebarang aktiviti pelanggaran.

Peranan:	MINDEFCERT / Unit Integriti

Kawalan:	Perkara:
A.2.1.4	**Hubungan Dengan Kumpulan Berkepentingan yang Khusus** *(Contact with Special Interest Groups)*

Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional ataupun forum bagi:

(i) Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat;
(ii) Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini;
(iii) Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan
(iv) Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.

Peranan:	Warga MINDEF (Mengikut Bidang Kepakaran)

Kawalan:	Perkara:
A.2.1.5	**Keselamatan Maklumat dalam Pengurusan Projek** *(Information Security in Project Management)*

Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek MINDEF;
(ii) Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek;
(iii) Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan;
(iv) Dokumen kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam Polisi Keselamatan Siber Kementerian Pertahanan Malaysia (PKS MINDEF) ; dan
(v) Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal yang mempunyai pensijilan keselamatan maklumat (mengikut keperluan)

Peranan:	Warga MINDEF (Pasukan Projek)

A.2.2 PERANTI MUDAH ALIH DAN TELEKERJA

(MOBILE DEVICES AND TELEWORKING)

Objektif: Memastikan keselamatan telekerja dan penggunaan peralatan mudah alih.

Kawalan:	Perkara:
A.2.2.1	**Polisi Peranti Mudah Alih** *(Mobile Device Policy)*

(i) **Bahagian Pengurusan Maklumat (BPM) MINDEF dan Bahagian Siber dan Elektromagnetik Pertahanan (BSEP)**

Membangun serta menyebarkan dasar dan langkah-langkah keselamatan sokongan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih.

Peranan:	BPM dan BSEP

(ii) **Jawatankuasa Pemandu ICT (JPICT) MINDEF**

Meluluskan dasar, arahan, peraturan dan langkah keselamatan berkaitan penggunaan peranti mudah alih ICT kepada warga MINDEF.

Peranan:	JPICT MINDEF

(iii) Warga MINDEF

Perkara-perkara yang perlu dipatuhi:

(a) Pendaftaran ke atas peralatan mudah alih;
(b) Keperluan ke atas perlindungan secara fizikal;
(c) Kawalan ke atas pemasangan perisian peralatan mudah alih;
(d) Kawalan ke atas versi dan *patches* perisian;
(e) Sekatan ke atas akses perkhidmatan maklumat secara dalam talian;
(f) Kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptografi;
(g) Peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan; dan
(h) Peralatan mudah alih hendaklah dipasang dengan perisian keselamatan *(antivirus, antimalware)*.

Peranan:	Warga MINDEF

Kawalan:	Perkara:
A.2.2.2	**Telekerja** *(Teleworking)*

Dasar dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi telekerja.

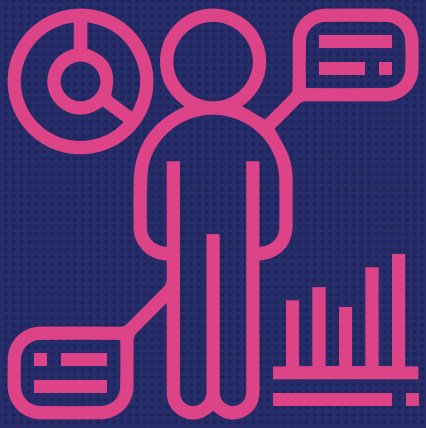
Peranan:	Warga MINDEF

BIDANG A.3

A.3.1 Sebelum Perkhidmatan *(Prior To Employment)* 37
A.3.1.1 Tapisan Keselamatan *(Security Screening)*
A.3.1.2 Terma dan Syarat Perkhidmatan *(Terms and Conditions of Employment)*

A.3.2 Dalam Tempoh Perkhidmatan *(During Employment)* 38
A.3.2.1 Tanggungjawab Pengurusan *(Management Responsibilities)*
A.3.2.2 Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat *(Information Security Awareness, Education and Training)*
A.3.2.3 Proses Tatatertib *(Disciplinary Process)*

A.3.3 Penamatan dan Pertukaran Perkhidmatan 40
(Termination and Change of Employment)
A.3.3.1 Penamatan atau Pertukaran Tanggungjawab Perkhidmatan *(Termination or Change of Employment Responsibilities)*



Keselamatan Sumber Manusia

Human Resource Security

A.3.1 SEBELUM PERKHIDMATAN *(PRIOR TO EMPLOYMENT)*

Objektif: **Memastikan warga MINDEF, pembekal, pakar runding dan pihak yang mengakses dan menggunakan perkhidmatan digital MINDEF memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT.**

Kawalan:	Perkara:
A.3.1.1	**Tapisan Keselamatan** *(Security Screening)*

Tapisan keselamatan hendaklah dijalankan terhadap warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF yang terlibat dalam menjamin keselamatan aset digital atau ICT sebelum, semasa dan selepas perkhidmatan; dan

(ii) Menjalankan tapisan keselamatan untuk warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.

(iii) Pihak pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF hendaklah menjalani Tapisan Keselamatan MINDEF serta Tapisan Keselamatan Ketua Pegawai Keselamatan Kerajaan (CGSO).

Peranan:	Ketua Jabatan, BKP, Warga MINDEF, pembekal, pakar runding dan pihak yang mengakses dan menggunakan perkhidmatan digital MINDEF

Kawalan:	Perkara:
A.3.1.2	**Terma dan Syarat Perkhidmatan** *(Terms and Conditions of Employment)*

Kontrak dengan warga, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut:

(i) Menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT MINDEF yang terlibat dalam menjamin keselamatan aset ICT; dan

(ii) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

Peranan:	Ketua Jabatan, Pentadbir Sistem, Pengguna dan Pembekal

A.3.2 DALAM TEMPOH PERKHIDMATAN

(DURING EMPLOYMENT)

Objektif: Memastikan warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.

Kawalan:	Perkara:
A.3.2.1	**Tanggungjawab Pengurusan** *(Management Responsibilities)*

Pihak pengurusan hendaklah memastikan warga, pembekal, pakar runding dan pihak yang mengakses dan menggunakan perkhidmatan digital MINDEF supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.

Peranan:	Warga, pembekal, pakar runding dan pihak yang mengakses dan menggunakan perkhidmatan digital MINDEF

Kawalan:	Perkara:
A.3.2.2	**Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat** *(Information Security Awareness, Education and Training)*

Warga, pembekal, pakar runding dan pihak yang mengakses dan menggunakan perkhidmatan digital MINDEF perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber MINDEF, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk / fungsi / aplikasi / sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka;

(ii) Memastikan kesedaran yang berkaitan Polisi Keselamatan Siber Kementerian Pertahanan (PKS MINDEF) perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan

(iii) Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.

Peranan:	Ketua Jabatan, Pentadbir Sistem, Pengguna dan Pembekal

Kawalan:	Perkara:
A.3.2.3	**Proses Tatatertib** *(Disciplinary Process)*

Proses tatatertib hendaklah ditetapkan bagi membolehkan tindakan diambil terhadap warga MINDEF yang melakukan pelanggaran keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga MINDEF sekiranya berlaku perlanggaran terhadap perundangan dan peraturan yang ditetapkan oleh MINDEF;

(ii) Warga MINDEF yang melanggar polisi ini dan didapati bersalah akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT MINDEF dan ATM.

Peranan:	Unit Integriti dan Perkhidmatan ATM

A.3.3 PENAMATAN DAN PERTUKARAN PERKHIDMATAN

(TERMINATION AND CHANGE OF EMPLOYMENT)

Objektif: Memastikan pertukaran, tamat perkhidmatan dan perubahan bidang tugas diurus dengan teratur.

Kawalan:	Perkara:
A.3.3.1	**Penamatan atau Pertukaran Tanggungjawab Perkhidmatan** *(Termination or Change of Employment Responsibilities)*

Warga yang telah tamat perkhidmatan perlu mematuhi perkara-perkara berikut:

(i) Memastikan semua aset ICT dikembalikan kepada BPM MINDEF/ Perkhidmatan ATM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan

(ii) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan MINDEF dan terma perkhidmatan yang ditetapkan.

(iii) Maklumat rasmi kerajaan dalam peranti tidak dibenarkan dibawa keluar dari premis MINDEF tanpa kebenaran.

Warga yang telah bertukar ke perkhidmatan/agensi lain hendaklah:

(i) Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada BPM MINDEF/ Perkhidmatan ATM mengikut peraturan dan terma perkhidmatan yang ditetapkan; dan

(ii) Menyedia dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.

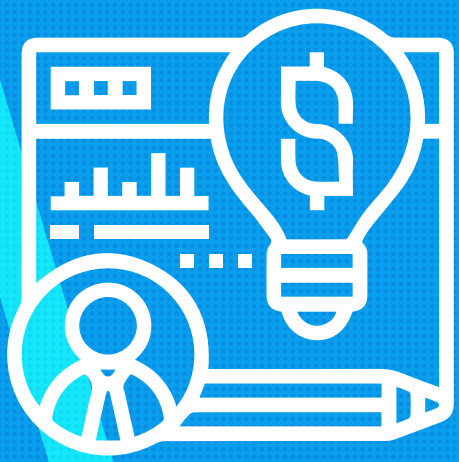
Peranan:	BPM MINDEF, Perkhidmatan ATM, Warga MINDEF

BIDANG A.4

A.4.1 Tanggungjawab Terhadap Aset *(Responsibility for Assets)* 43
- A.4.1.1 Inventori Aset *(Inventory of Assets)*
- A.4.1.2 Pemilikan Aset *(Ownership of Assets)*
- A.4.1.3 Penggunaan Aset yang Dibenarkan *(Acceptable Use of Assets)*
- A.4.1.4 Pemulangan Aset *(Return of Assets)*

A.4.2 Pengelasan Maklumat *(Classification of Information)* 44
- A.4.2.1 Pengelasan Maklumat *(Classification of Information)*
- A.4.2.2 Pelabelan Maklumat *(Labelling of Information)*
- A.4.2.3 Pengendalian Aset *(Handling of Assets)*

A.4.3 Pengendalian Media *(Media Handling)* 46
- A.4.3.1 Pengurusan Media Boleh Alih *(Management of Removal Media)*
- A.4.3.2 Pelupusan Media *(Disposal of Media)*
- A.4.3.3 Pemindahan Media Fizikal *(Physical Media Transfer)*



Pengurusan Aset

Asset Management

A.4.1 TANGGUNGJAWAB TERHADAP ASET

(RESPONSIBILITY FOR ASSETS)

Objektif: Untuk mengenal pasti aset bagi memberikan dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MINDEF.

Kawalan:	Perkara:
A.4.1.1	**Inventori Aset** *(Inventory of Assets)*

Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT MINDEF. Aset-aset ICT MINDEF hendaklah diuruskan mengikut Tatacara Pengurusan Aset yang berkuatkuasa.

Peranan:	Pegawai Penerima Aset, Pegawai Aset dan Warga MINDEF

Kawalan:	Perkara:
A.4.1.2	**Pemilikan Aset** *(Ownership of Assets)*

Aset yang boleh diselenggara hanyalah aset hak milik MINDEF. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara-perkara berikut:

i) Memastikan aset di bawah tanggungjawabnya telah dimasukkan dalam senarai aset;
(ii) Memastikan aset telah dikelaskan dan dilindungi;
(iii) Mengenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan;
(iv) Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan
(v) Memastikan semua jenis aset dipelihara dengan baik.

Peranan:	Pegawai Aset dan Warga MINDEF

Kawalan:	Perkara:
A.4.1.3	**Penggunaan Aset yang Dibenarkan** *(Acceptable Use of Assets)*

Warga MINDEF hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak.

Peranan:	Warga MINDEF

A.4.2 PENGELASAN MAKLUMAT

(CLASSIFICATION OF INFORMATION)

Objektif: Untuk mengenal pasti aset bagi memberikan dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MINDEF.

Kawalan:	Perkara:
A.4.2.1	**Pengelasan Maklumat** *(Classification of Information)*

Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan.

Peranan:	Pegawai Pengelas

Kawalan:	Perkara:
A.4.2.2	**Pelabelan Maklumat** *(Labelling of Information)*

Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan.

Peranan:	Warga MINDEF

Kawalan:	Perkara:
A.4.2.3	**Pengendalian Aset** *(Handling of Assets)*

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut:

(i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
(ii) Memeriksa dan menentukan maklumat adalah tepat dan lengkap dari semasa ke semasa;
(iii) Menentukan maklumat sedia untuk digunakan;
(iv) Menjaga kerahsiaan kata laluan;
(v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
(vi) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, membuat salinan, penghantaran, penyampaian, pertukaran dan pemusnahan;
(vii) Memastikan maklumat terperingkat yang disimpan di dalam storan dalaman atau luaran (*internal* atau *external hardisk*) diberi perlindungan melalui kaedah enkripsi yang bersesuaian; dan
(viii) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.

Peranan:	Warga MINDEF

A.4.3 PENGENDALIAN MEDIA *(MEDIA HANDLING)*

Objektif: Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

Kawalan:	Perkara:
A.4.3.1	**Pengurusan Media Boleh Alih** *(Management of Removal Media)*

Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh MINDEF. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut:

(i) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;
(ii) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;
(iii) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;
(iv) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan
(v) Menyimpan semua jenis media di tempat yang selamat.

Peranan:	Pentadbir Sistem ICT dan Pengguna

Kawalan:	Perkara:
A.4.3.2	**Pelupusan Media** *(Disposal of Media)*

Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan.

Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.

Peranan:	Pentadbir Sistem ICT dan Jawatankuasa yang dilantik untuk pelupusan aset.

Kawalan:	Perkara:
A.4.3.3	**Pemindahan Media Fizikal** *(Physical Media Transfer)*

Media yang mengandungi maklumat perlu dilindungi daripada akses tanpa izin, penyalahgunaan atau kerosakan semasa dipindahkan. Media yang dimaksudkan juga adalah termasuk dokumen dalam bentuk kertas.

Perkara-perkara berikut perlu dipertimbangkan semasa pemindahan dilakukan seperti berikut:

(i) Perkhidmatan pengangkutan atau kurier yang boleh dipercayai digunakan;
(ii) Senarai kurier yang digunakan perlu mendapat persetujuan Ketua Jabatan;
(iii) Pembungkusan perlu mencukupi bagi melindungi kerosakan fizikal yang mungkin timbul semasa transit; dan
(iv) Rekod atau log perlu disimpan untuk mengenalpasti kandungan media, perlindungan yang digunakan serta rakaman semasa pemindahan kepada penjaga transit dan penerimaan di destinasi.

Pemindahan dokumen terperingkat secara fizikal pula perlu mengikut prosedur-prosedur seperti di dalam Arahan Keselamatan.

Peranan:	Warga MINDEF, Ketua Jabatan

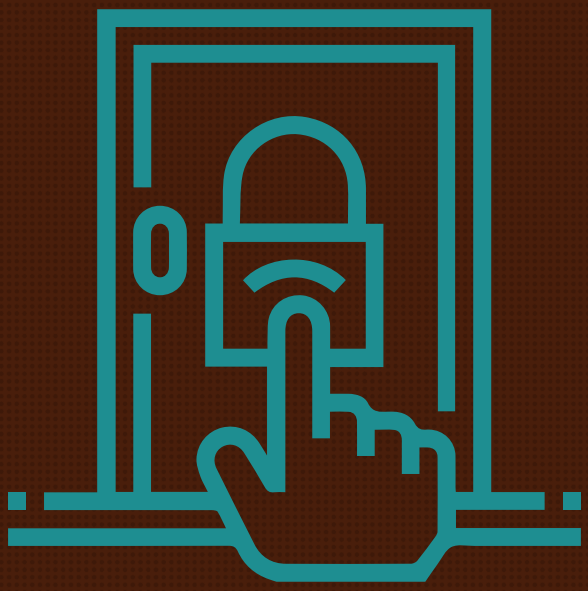
BIDANG A.5

A.5.1 Keperluan Kawalan Akses *(Business Requirements of Access Control)* 51
- A.5.1.1 Polisi Kawalan Akses *(Access Control Policy)*
- A.5.1.2 Capaian Kepada Rangkaian dan Perkhidmatan Rangkaian *(Access to Networks and Network Services)*

A.5.2 Pengurusan Akses Pengguna *(User Access Management)* 53
- A.5.2.1 Pendaftaran dan Pembatalan Pengguna *(User Registration and Deregistration)*
- A.5.2.2 Peruntukan Akses Pengguna *(User Access Provisioning)*
- A.5.2.3 Pengurusan Hak Akses Istimewa *(Management of Privileged Access Rights)*
- A.5.2.4 Pengurusan Maklumat Pengesahan Rahsia Pengguna *(Management of Secret Authentication Information of Users)*
- A.5.2.5 Kajian Semula Hak Akses Pengguna *(Review of User Access Rights)*
- A.5.2.6 Pembatalan atau Pelarasan Hak Akses *(Removal or Adjustment of Access Rights)*

A.5.3 Tanggungjawab Pengguna *(User Responsibilities)* 56
- A.5.3.1 Pengurusan Maklumat Pengesahan Rahsia Pengguna *(Management of Secret Authentication Information of Users)*
- A.5.3.2 Penggunaan Maklumat Pengesahan Rahsia *(Use of Secret Authentication Information)*

A.5.4 Kawalan Akses Sistem dan Aplikasi *(System and Application Access Control)* 57
- A.5.4.1 Sekatan Akses Maklumat *(Information Access Restriction)*
- A.5.4.2 Prosedur Log Masuk yang Selamat *(Secure Log-On Procedure)*
- A.5.4.3 Sistem Pengurusan Kata Laluan *(Password Management System)*
- A.5.4.4 Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa *(Use of Privileged Utility Programs)*
- A.5.4.5 Kawalan Akses Kepada Kod Sumber Program *(Access Control to Program Source Code)*



Kawalan Akses

Access Control

A.5.1 KEPERLUAN KAWALAN AKSES

(BUSINESS REQUIREMENTS OF ACCESS CONTROL)

Objektif: **Menghadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.**

Kawalan:	Perkara:
A.5.1.1	**Polisi Kawalan Akses** *(Access Control Policy)*

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza.

Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. la perlu dikemas kini setahun sekali atau mengikut keperluan semasa dan menyokong peraturan kawalan capaian pengguna sedia ada. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Keperluan keselamatan aplikasi;
(ii) Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian;
(iii) Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa;
(iv) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;
(v) Pengasingan peranan kawalan capaian;
(vi) Kebenaran rasmi permintaan akses;
(vii) Keperluan semakan hak akses berkala;
(viii) Pembatalan hak akses;
(ix) Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan
(x) Keistimewaan akses *(access privilege)*.

Peranan:	Pemilik Perkhidmatan Digital / Pentadbir Sistem ICT

Kawalan:	Perkara:
A.5.1.2	**Capaian kepada Rangkaian dan Perkhidmatan Rangkaian** *(Access to Networks and Network Services)*

Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari Pentadbir Rangkaian MINDEF. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

(i) Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian MINDEF, rangkaian agensi lain dan rangkaian awam;

(ii) Mewujud dan menguatkuasakan mekanisme pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan

(iii) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.

Peranan:	ICTSO / Pengurus ICT / Pentadbir Rangkaian

A.5.2 PENGURUSAN AKSES PENGGUNA

(USER ACCESS MANAGEMENT)

Objektif: Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.

Kawalan:	Perkara:
A.5.2.1	**Pendaftaran dan Pembatalan Pengguna** *(User Registration and Deregistration)*

Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara-perkara berikut hendaklah dipatuhi:

(i) Akaun yang diperuntukkan oleh MINDEF sahaja boleh digunakan;
(ii) Akaun pengguna mestilah unik;
(iii) Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada MINDEF terlebih dahulu;
(iv) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;
(v) Pemilikan akaun bukanlah hak mutlak pengguna dan boleh ditarik balik jika penggunaannya melanggar peraturan MINDEF; dan
(vi) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan MINDEF dan didokumentasikan.

Peranan:	Pentadbir Sistem ICT / Pengguna

Kawalan:	Perkara:
A.5.2.2	**Peruntukan Akses Pengguna** *(User Access Provisioning)*

Proses formal peruntukan akses pengguna perlu dilaksanakan dalam pemberian atau pembatalan hak akses kepada semua jenis pengguna termasuk sistem dan perkhidmatan.

Proses peruntukan untuk memberi atau membatalkan hak akses yang diberikan kepada ID Pengguna perlu merangkumi :

i) Mendapatkan kebenaran daripada pemilik sistem atau perkhidmatan ICT;
ii) Menentusahkan tahap akses yang diberikan adalah wajar dan selaras dengan keperluan tugas;
iii) Memastikan hak akses tidak diaktifkan sebelum prosedur kebenaran dilengkapkan;
iv) Mengekalkan rekod berpusat untuk hak akses yang diberikan kepada ID Pengguna;
v) Menyesuaikan hak akses pengguna yang menukar peranan atau pekerjaan dan segera menyekat atau menghapuskan hak akses pengguna yang telah meninggalkan organisasi; dan
vi) Mengkaji semula secara berkala hak akses tersebut.

Peranan:	Pentadbir Sistem ICT / Pengarah Bahagian

Kawalan:	Perkara:
A.5.2.3	**Pengurusan Hak Akses Istimewa** *(Management of Privileged Access Rights)*

Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal.

Penetapan dan penggunaan ke atas hak akses perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas merujuk kepada prosedur pendaftaran dan penamatan pengguna.

Peranan:	Pentadbir Sistem ICT

Kawalan:	Perkara:
A.5.2.4	**Pengurusan Maklumat Pengesahan Rahsia Pengguna** *(Management of Secret Authentication Information of Users)*

Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.

Peranan:	Pentadbir Sistem ICT

Kawalan:	Perkara:
A.5.2.5	**Kajian Semula Hak Akses Pengguna** *(Review of User Access Rights)*

Pemilik aset hendaklah menyemak hak akses pengguna pada sela masa yang ditetapkan.

Pentadbir Sistem ICT perlu mewujudkan Prosedur Pendaftaran dan Penamatan Pengguna sistem masing-masing sebagai rujukan semakan ke atas hak akses pengguna pada sela masa yang ditetapkan.

Peranan:	Pentadbir Sistem ICT

Kawalan:	Perkara:
A.5.2.6	**Pembatalan atau Pelarasan Hak Akses** *(Removal or Adjustment of Access Rights)*

Hak akses kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikemaskini mengikut keperluan semasa.

Peranan:	Pentadbir Sistem ICT / Pengurus ICT

A.5.3 TANGGUNGJAWAB PENGGUNA
(USER RESPONSIBILITIES)

Objektif: Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka.

Kawalan:	Perkara:
A.5.3.1	**Pengurusan Maklumat Pengesahan Rahsia Pengguna** *(Management of Secret Authentication Information of Users)*

Peranan dan tanggungjawab pengguna adalah seperti yang berikut:

(i) Membaca, memahami dan mematuhi Polisi Keselamatan Siber Kementerian Pertahanan (PKS MINDEF);
(ii) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya;
(iii) Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat MINDEF;
(iv) Melaksanakan langkah-langkah perlindungan seperti yang berikut:
    (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
    (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
    (c) Menentukan maklumat sedia untuk digunakan;
    (d) Menjaga kerahsiaan kata laluan;
    (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
    (f) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
    (g) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.
(v) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera; dan
(vi) Menghadiri program-program kesedaran mengenai keselamatan siber.

Peranan:	Pengguna, Pentadbir Sistem ICT / Pengurus ICT

Kawalan:	Perkara:
A.5.3.2	**Penggunaan Maklumat Pengesahan Rahsia** *(Use of Secret Authentication Information)*

Pengguna perlu mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti.

Peranan:	Pentadbir Sistem ICT / Pengguna

A.5.4 KAWALAN AKSES SISTEM DAN APLIKASI

(SYSTEM AND APPLICATION ACCESS CONTROL)

Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke alas maklumat yang terdapat di dalam sistem dan aplikasi.

Kawalan:	Perkara:
A.5.4.1	**Sekatan Akses Maklumat** *(Information Access Restriction)*

Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian.

Peranan:	Pentadbir Sistem ICT / Pengguna

Kawalan:	Perkara:
A.5.4.2	**Prosedur Log Masuk yang Selamat** *(Secure Log-On Procedure)*

Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan adalah seperti yang berikut:

(i) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan MINDEF;

(ii) Menjana amaran *(alert)* sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem;

(iii) Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin;

(iv) Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna;

(v) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti;

(vi) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.

Peranan:	Pentadbir Sistem ICT

Kawalan:	Perkara:
A.5.4.3	**Sistem Pengurusan Kata Laluan** *(Password Management System)*

Sistem pengurusan kata laluan hendaklah interaktif dan mengambilkira kualiti kata laluan yang dicipta. Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MINDEF seperti yang berikut:

(i) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;
(ii) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;
(iii) Panjang kata laluan mestilah sekurang-kurangnya **DUA BELAS (12) AKSARA** dengan gabungan antara huruf, aksara khas dan nombor *(alphanumeric)* KECUALI bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad.
(iv) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekali pun;
(v) Kata laluan paparan kunci *(lock screen)* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;
(vi) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara;
(vii) Kuatkuasakan pertukaran kata laluan semasa atau selepas login kali pertama atau selepas reset kata laluan;
(viii) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;
(ix) Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum **TIGA (3) KALI** sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; dan
(x) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.

Peranan:	Pentadbir Sistem ICT / Pengguna

Kawalan:	Perkara:
A.5.4.4	**Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa** *(Use of Privileged Utility Programs)*

Penggunaan program utiliti hendaklah dikawal bagi mengelakkan *Over-Riding* sistem.

Peranan:	Pengurus ICT / Pentadbir Sistem ICT

Kawalan:	Perkara:
A.5.4.5	**Kawalan Akses Kepada Kod Sumber Program** *(Access Control to Program Source Code)*

Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Log audit perlu dikekalkan kepada semua akses kepada kod sumber;
(ii) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan
(iii) Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik MINDEF.

Peranan:	Pengarah Projek / Pengurus Projek / Pentadbir Sistem ICT

BIDANG A.6

A.6.1 Kawalan Kriptografi *(Cryptography Controls)* 63
A.6.1.1 Dasar Kriptografi *(Cryptography Policy)*
A.6.1.2 Pengurusan Kunci Awam *(Public Key Management)*
A.6.1.3 Tandatangan Digital *(Digital Signature)*

Kriptografi

Cryptography

A.6.1 KAWALAN KRIPTOGRAFI *(CRYPTOGRAPHY CONTROLS)*

Objektif: Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, kesahihan dan keutuhan maklumat.

Kawalan:	Perkara:
A.6.1.1	**Dasar Kriptografi** *(Cryptography Policy)*

Kriptografi merangkumi kaedah-kaedah seperti yang berikut:

(i) 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; dan

(ii) 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 di akses oleh Kerajaan bagi tujuan kawalan, penilaian dan analisa keselamatan.

Peranan:	ICTSO, Pengurus ICT

Kawalan:	Perkara:
A.6.1.2	**Pengurusan Kunci Awam** *(Public Key Management)*

Pengurusan Infrastruktur Kunci Awam/*Public Key Infrastructure* (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.

(i) Semua kunci kriptografi yang dihasilkan bagi melindungi maklumat terperingkat adalah hak milik Kerajaan;

(ii) Kunci kriptografi mestilah diuruskan, diselia dan dilindungi dengan menggunakan kaedah yang ditetapkan dan hendaklah dirahsiakan;

(iii) Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut.

Peranan:	ICTSO, Pentadbir Sistem, Pengguna

Kawalan:	Perkara:
A.6.1.3	**Tandatangan Digital** *(Digital Signature)*

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.

Peranan:	Pentadbir Sistem, Pengguna

BIDANG A.7

A.7.1 Kawasan Selamat *(Secure Areas)* 67

- A.7.1.1 Perimeter Keselamatan Fizikal *(Physical Security Parameter)*
- A.7.1.2 Kawalan Kemasukan Fizikal *(Physical Entry Controls)*
- A.7.1.3 Keselamatan Pejabat, Bilik dan Kemudahan *(Securing Offices, Rooms and Facilities)*
- A.7.1.4 Perlindungan Daripada Ancaman Luar Dan Persekitaran *(Protecting Against External and Environmental Threats)*
- A.7.1.5 Bekerja di Kawasan Selamat *(Working in Secure Areas)*
- A.7.1.6 Kawasan Penyerahan dan Pemunggahan *(Delivery and Loading Areas)*

A.7.2 Peralatan ICT *(ICT Equipment)* 70

- A.7.2.1 Penempatan dan Perlindungan Peralatan ICT *(Equipment Sitting and Protection)*
- A.7.2.2 Utiliti Sokongan *(Supporting Utilities)*
- A.7.2.3 Keselamatan Kabel *(Cabling Security)*
- A.7.2.4 Penyenggaraaan Peralatan *(Equipment Maintenance)*
- A.7.2.5 Pengalihan Aset *(Removal of Assets)*
- A.7.2.6 Keselamatan Peralatan dan Aset di Luar Premis *(Security of Equipment Off-Premises)*
- A.7.2.7 Pelupusan yang Selamat atau Penggunaan Semula Peralatan *(Secure Disposal or Re-Use of Equipment)*
- A.7.2.8 Peralatan Pengguna Tanpa Kawalan *(Unattended User Equipment)*
- A.7.2.9 Dasar Meja Kosong dan Skrin Kosong *(Clear Desk dan Clear Screen Policy)*

Keselamatan Fizikal Dan Persekitaran

Physical And Environmental Security

A.7.1 KAWASAN SELAMAT *(SECURE AREAS)*

Objektif: Menghalang akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat MINDEF.

Kawalan:	Perkara:
A.7.1.1	**Perimeter Keselamatan Fizikal** *(Physical Security Parameter)*

Perimeter keselamatan hendaklah ditakrifkan dan digunakan untuk melindungi Kawasan Larangan dan Tempat Larangan yang mengandungi maklumat sensitif atau kritikal dan juga kemudahan pemprosesan maklumat.

Ini bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan Aset ICT MINDEF. Perkara-perkara yang perlu dipatuhi perlu selaras dengan Akta Kawasan Larangan dan Tempat Larangan serta Arahan Keselamatan yang berkuatkuasa.

Peranan:	BKP, Ketua Jabatan

Kawalan:	Perkara:
A.7.1.2	**Kawalan Kemasukan Fizikal** *(Physical Entry Controls)*

Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis MINDEF. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Setiap pegawai dan kakitangan MINDEF hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan kepada MINDEF apabila bertukar, tamat perkhidmatan atau bersara;
(ii) Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan;
(iii) Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan Aset ICT MINDEF;dan
(iv) Kehilangan pas hendaklah dilaporkan segera kepada Pihak Berkuasa.

Peranan:	Warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF

Kawalan:	Perkara:
A.7.1.3	**Keselamatan Pejabat, Bilik dan Kemudahan** *(Securing Offices, Rooms and Facilities)*

Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Kawasan tempat bekerja, bilik mesyuarat, bilik krisis, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan CCTV dan pusat data atau bilik server dan bilik yang menempatkan perkakasan rangkaian perlu dihadkan daripada diakses tanpa kebenaran;

(ii) Kawasan tempat berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar;

(iii) Pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF yang diberi akses ke ruang operasi ICT, pusat data atau bilik server dan bilik rangkaian hendaklah diiringi oleh wakil MINDEF sepanjang masa; dan

(iv) Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi Arahan Keselamatan.

Peranan:	Warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF.

Kawalan:	Perkara:
A.7.1.4	**Perlindungan Daripada Ancaman Luar Dan Persekitaran** *(Protecting Against External and Environmental Threats)*

Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. MINDEF perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.

Peranan:	Pentadbir Pusat Data dan BKP

Kawalan:	Perkara:
A.7.1.5	**Bekerja di Kawasan Selamat** *(Working in Secure Areas)*

Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga MINDEF yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis MINDEF termasuklah Pusat Data.

Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas kawasan tersebut adalah seperti yang berikut:

(i) Sumber data atau *server*, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran;
(ii) Akses adalah terhad kepada warga MINDEF yang telah diberi kuasa sahaja dan dipantau pada setiap masa;
(iii) Pemantauan dibuat menggunakan *Closed-Circuit Television* (CCTV) kamera atau lain-lain peralatan yang sesuai;
(iv) Peralatan keselamatan (CCTV, log akses) perlu diperiksa dan disenggara secara berjadual;
(v) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan;
(vi) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan;
(vii) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam;
(viii) Memperkukuh tingkap dan pintu serta dikunci sepanjang masa untuk mengawal kemasukan;
(ix) Memperkukuh dinding dan siling; dan
(x) Menghadkan jalan keluar masuk.

Peranan:	Pentadbir Pusat Data dan BKP

Kawalan:	Perkara:
A.7.1.6	**Kawasan Penyerahan dan Pemunggahan** *(Delivery and Loading Areas)*

Titik kemasukan / *access point* seperti kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan.

MINDEF hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.

Peranan:	Warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF.

A.7.2 PERALATAN ICT *(ICT EQUIPMENT)*

Objektif: Melindungi peralatan ICT MINDEF daripada kehilangan, kerosakan, kecurian dan disalahgunakan.

Kawalan:	Perkara:
A.7.2.1	**Penempatan dan Perlindungan Peralatan ICT** *(Equipment Sitting and Protection)*

Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut:

(i) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

(ii) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;

(iii) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;

(iv) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem;

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

(vi) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna;

(vii) Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya;

(viii) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set* (Gen-Set);

(ix) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan.

(x) Peralatan rangkaian seperti *switch*, *router*, *hub* dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci;

(xi) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan *(air ventilation)* yang sesuai;

(xii) Peralatan ICT yang hendak dibawa ke luar premis MINDEF, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan;

(xiii) Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

(xiv) Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal;
(xv) Pengguna dilarang sama sekali mengubah *password* bagi akaun *administrator* yang telah ditetapkan oleh Pentadbir Sistem ICT; dan
(xvi) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi sahaja.

Peranan:	Warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF.

Kawalan:	Perkara:
A.7.2.2	**Utiliti Sokongan** *(Supporting Utilities)*

Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Semua alat sokongan perlu diselenggara dari semasa ke semasa (sekurang-kurangnya setahun sekali).

Laporan senggaraan perlu disahkan dan disemak dan jika terdapat cadangan pembaikan atau penggantian komponen mahupun perkakasan, pihak bertanggungjawab ke atas perkakasan tersebut perlu melaksanakannya dengan kadar segera.

Peranan:	Warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF.

Kawalan:	Perkara:
A.7.2.3	**Keselamatan Kabel** *(Cabling Security)*

Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut:

(i) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;
(ii) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;
(iii) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan
(iv) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* atau *tray* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.

Peranan:	Pentadbir Sistem ICT

Kawalan:	Perkara:
A.7.2.4	**Penyenggaraaan Peralatan** *(Equipment Maintenance)*

Peralatan ICT hendaklah disenggara dengan betul dan berkala bagi memastikan ketersediaan dan keutuhannya berterusan. Perkakasan hendaklah disenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut:

(i) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;
(ii) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara;
(iii) Memastikan perkakasan hanya disenggara oleh kakitangan atau pihak yang dibenarkan sahaja;
(iv) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyenggaraan; dan
(v) Memaklumkan pihak pengguna sebelum melaksanakan penyenggaraan mengikut jadual yang ditetapkan atau atas keperluan.

Peranan:	Pegawai Aset, Pentadbir Sistem ICT

Kawalan:	Perkara:
A.7.2.5	**Pengalihan Aset** *(Removal of Assets)*

Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut:

(i) Peralatan ICT yang hendak dibawa keluar dari premis MINDEF untuk tujuan rasmi, perlulah mendapat kelulusan KSU atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan
(ii) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.

Peranan:	Pengguna, Pegawai Aset

Kawalan:	Perkara:
A.7.2.6	**Keselamatan Peralatan dan Aset di Luar Premis** *(Security of Equipment Off-Premises)*

Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis MINDEF.

Peralatan yang dibawa keluar dari premis MINDEF adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Peralatan perlu dilindungi dan dikawal sepanjang masa;
(ii) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan
(iii) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.

Peranan:	Warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF.

Kawalan:	Perkara:
A.7.2.7	**Pelupusan yang Selamat atau Penggunaan Semula Peralatan** *(Secure Disposal or Re-Use of Equipment)*

Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti *(overwrite)* sebelum dilupuskan atau diguna semula.

Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MINDEF dan ditempatkan di MINDEF.

Peralatan ICT yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuat kuasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan MINDEF. Langkah-langkah seperti yang berikut hendaklah diambil:

(i) Bagi peralatan ICT yang akan dilupuskan sebelum dipindah-milik, data-data dalam storan hendaklah dipastikan telah dihapuskan atau disanitasi dengan cara yang selamat mengikut Arahan Keselamatan yang berkuatkuasa;
(ii) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;
(iii) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;
(iv) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;

(v) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti yang berikut:
   (a) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan menjadi hak milik peribadi.
   (b) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti *RAM*, *Hardisk*, *Motherboard* dan sebagainya.
   (c) Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di MINDEF.
   (d) Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan;
   (e) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab MINDEF.

(vi) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti *thumbdrive* atau *external hardisk* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan;

(vii) Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal. Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan;

(viii) Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang berkuat kuasa;

(ix) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Arkib Negara; dan

(x) Pegawai aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori.

Peranan:	Pegawai Aset, Pentadbir Sistem ICT dan warga MINDEF

Kawalan:	Perkara:
A.7.2.8	**Peralatan Pengguna Tanpa Kawalan** *(Unattended User Equipment)*

Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut:

(i) Tamatkan sesi aktif apabila selesai tugas;

(ii) *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan

(iii) Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.

Peranan:	Warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF.

Kawalan:	Perkara:
A.7.2.9	**Dasar Meja Kosong dan Skrin Kosong** *(Clear Desk dan Clear Screen Policy)*

Dasar meja kosong untuk kertas dan media penyimpanan boleh alih serta dasar skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

Clear Desk bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.

Langkah-langkah yang perlu diambil termasuklah seperti yang berikut:

(i) Menggunakan kemudahan *password screensaver* atau *logout* apabila meninggalkan komputer;
(ii) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci;
(iii) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotokopi.
(iv) E-mel masuk dan keluar hendaklah dikawal; dan
(v) Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.

Peranan:	Warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF.

BIDANG A.8

A.8.1 Prosedur dan Tanggungjawab Operasi *(Operational Procedures Responsibilities)* 79
A.8.1.1 Pengendalian Prosedur Operasi *(Handling of Operational Procedures)*
A.8.1.2 Pengurusan Perubahan *(Change Management)*
A.8.1.3 Pengurusan Kapasiti *(Capacity Management)*
A.8.1.4 Pengasingan Kemudahan Pembangunan, Ujian dan Operasi *(Segregation of Development, Testing and Operational Environment)*

A.8.2 Perlindungan daripada Malware *(Protection from Malware)* 82
A.8.2.1 Kawalan Daripada Malware *(Controls Against Malware)*

A.8.3 Sandaran *(Backup)* 83
A.8.3.1 Sandaran Maklumat *(Information Backup)*

A.8.4 Log dan Pemantauan *(Logging and Monitoring)* 84
A.8.4.1 Log Kejadian dan Perlindungan Maklumat Log *(Event Log and Protection of Log Information)*
A.8.4.2 Penyeragaman Masa *(Time Synchronization)*

A.8.5 Pengurusan Kerentanan Teknikal *(Technical Vulnerability Management)* 85
A.8.5.1 Pengurusan Kerentanan Teknikal *(Management of Technical Vulnerability)*
A.8.5.2 Sekatan Ke Atas Pemasangan Perisian *(Restriction on Software Installation)*

A.8.6 Pertimbangan Tentang Audit Sistem *(Systems Audit Considerations)* 86
A.8.6.1 Kawalan Audit Sistem Maklumat *(Information Systems Audit Controls)*

Keselamatan Operasi

Operations Security

A.8.1 PROSEDUR DAN TANGGUNGJAWAB OPERASI

(OPERATIONAL PROCEDURES AND RESPONSIBILITIES)

Objektif: **Memastikan pengurusan operasi pemprosesan maklumat dilaksanakan dengan cekap dan selamat.**

Kawalan:	Perkara:
A.8.1.1	**Pengendalian Prosedur Operasi** *(Handling of Operational Procedures)*

Semua prosedur pengurusan operasi hendaklah dikenal pasti, didokumenkan, disimpan dan dihadkan capaian berdasarkan keperluan.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(i) Semua prosedur operasi hendaklah didokumenkan dengan jelas, teratur, dikemaskinikan dan sedia digunapakai oleh pengguna;
(ii) Setiap perubahan kepada prosedur operasi mestilah dikawal;
(iii) Tugas dan tanggungjawab fungsi perlu diasingkan bagi mengurangkan risiko kecuaian dan penyalahgunaan aset ICT MINDEF; dan
(iv) 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.

Peranan:	Pengurus ICT, Pentadbir Sistem ICT

Kawalan:	Perkara:
A.8.1.2	**Pengurusan Perubahan** *(Change Management)*

Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara berikut:

(i) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;
(ii) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;
(iii) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan
(iv) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja.

Peranan:	Pemilik Sistem, Pentadbir Sistem ICT

Kawalan:	Perkara:
A.8.1.3	**Pengurusan Kapasiti** *(Capacity Management)*

Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan
(ii) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

Peranan:	Pengurus ICT, Pentadbir Sistem ICT

Kawalan:	Perkara:
A.8.1.4	**Pengasingan Kemudahan Pembangunan, Ujian dan Operasi** *(Segregation of Development, Testing and Operational Environment)*

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan dalam pengoperasian sebenar *(production environment)*.

(ii) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan

(iii) Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.

Peranan:	Pengurus ICT, Pentadbir Sistem ICT

A.8.2 PERLINDUNGAN DARIPADA *MALWARE*

(PROTECTION FROM MALWARE)

Objektif: Untuk memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada *malware*.

Kawalan:	Perkara:
A.8.2.1	**Kawalan Daripada Malware** *(Controls Against Malware)*

Aset ICT perlu dilindungi supaya tidak terdedah kepada kerosakan yang disebabkan oleh kod hasad seperti *virus*, *worm*, *trojan* dan seumpamanya. Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan *malware* hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut.

Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya adalah seperti berikut:

(i) Memasang sistem keselamatan untuk mengesan perisian hasad atau *malware* seperti antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat;

(ii) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;

(iii) Mengimbas semua perisian atau sistem dengan *antivirus* sebelum menggunakannya;

(iv) Mengemaskini *antivirus* dengan *signature/pattern antivirus* yang terkini;

(v) Mengemaskini *patches* sistem pengoperasian pada peralatan ICT;

(vi) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;

(vii) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;

(viii) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;

(ix) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan;

(x) Memberi amaran mengenai ancaman seperti serangan *virus* terhadap keselamatan aset ICT MINDEF;

(xi) Melaksanakan Program Kesedaran Pengguna yang bersesuaian; dan

(xii) Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.

Peranan:	ICTSO, Pentadbir Sistem ICT, Pengguna

A.8.3 SANDARAN *(BACKUP)*

Objektif: Melindungi kehilangan data.

Kawalan:	Perkara:
A.8.3.1	**Sandaran Maklumat** *(Information Backup)*

Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di *offsite*. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau sebelum melaksanakan sebarang kemaskini/ penaiktarafan yang kritikal;

(ii) Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi;

(iii) Menguji sistem sandaran sedia ada bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana; dan

(iv) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara **harian, mingguan, bulanan atau tahunan**. Kekerapan sandaran bergantung pada tahap kritikal maklumat, dan hendaklah disimpan sekurang-kurangnya **TIGA (3) GENERASI**.

Peranan:	Pentadbir Sistem ICT

A.8.4 LOG DAN PEMANTAUAN *(LOGGING AND MONITORING)*

Objektif: **Merekodkan peristiwa dan menghasilkan bukti.**

Kawalan:	Perkara:
A.8.4.1	**Log Kejadian dan Perlindungan Maklumat Log** *(Event Log and Protection of Log Information)*

Semua peristiwa dan bukti kewujudan insiden hendaklah direkodkan untuk tujuan jejak audit. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(i) Setiap sistem mestilah dimanfaatkan upaya fail jejaknya. Jenis fail jejak yang perlu diaktifkan adalah seperti yang berikut:

a) Fail log sistem pengoperasian;

b) Fail log servis (contoh: *web*, emel);

c) Fail log aplikasi (*audit trail*); dan

d) Fail log rangkaian (contoh: *switch*, *firewall*, IPS).

(ii) Mewujudkan prosedur untuk memantau penggunaan kemudahan memproses maklumat dan dipantau secara berkala;

(iii) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;

(iv) Maklumat log perlu dilindungi daripada sebarang ubahsuai dan capaian yang tidak dibenarkan;

(v) Sebarang kesalahan, kesilapan atau penyalahgunaan sistem perlu direkodkan, dianalisis dan diambil tindakan sewajarnya;

(vi) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera;

(vii) Semua perkakasan ICT MINDEF perlu diselaraskan dengan satu sumber masa yang piawai; dan

(viii) Sebarang aktiviti tidak sah seperti kecurian maklumat dan pencerobohan hendaklah dilaporkan kepada MINDEFCERT atau CERT agensi.

Peranan:	ICTSO, Pentadbir Sistem ICT

Kawalan:	Perkara:
A.8.4.2	**Penyeragaman Masa** *(Time Synchronizations)*

Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal.

Sistem sumber rujukan masa tunggal yang digunakan hendaklah dipastikan merujuk kepada sistem masa yang sah dan berintegriti.

Peranan:	Pentadbir Sistem ICT

A.8.5 PENGURUSAN KERENTANAN TEKNIKAL

(TECHNICAL VULNERABILITY MANAGEMENT)

Objektif: Memastikan kawalan kerentanan teknikal adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.

Kawalan:	Perkara:
A.8.5.1	**Pengurusan Kerentanan Teknikal** *(Management of Technical Vulnerability)*

Kerentanan sistem operasi dan aplikasi yang digunakan perlu dikawal dengan berkesan. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Melaksanakan ujian penembusan sekurang-kurangnya setahun sekali untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi sedia ada;
(ii) Memastikan sistem baharu dilaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal sistem aplikasi dan operasi sebelum memulakan pengoperasian;
(iii) Menganalisis tahap risiko kerentanan; dan
(iv) Mengambil tindakan pengolahan dan kawalan risiko.

Peranan:	Pentadbir Sistem ICT

Kawalan:	Perkara:
A.8.5.2	**Sekatan Ke Atas Pemasangan Perisian** *(Restriction on Software Installation)*

Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:

(i) Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF;
(ii) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; dan
(iii) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.

Peranan:	Pentadbir Sistem ICT, warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF

A.8.6 PERTIMBANGAN TENTANG AUDIT SISTEM

(SYSTEMS AUDIT CONSIDERATIONS)

Objektif: Meminimumkan kesan aktiviti audit terhadap sistem yang beroperasi.

Kawalan:	Perkara:
A.8.6.1	**Kawalan Audit Sistem Maklumat** *(Information Systems Audit Controls)*

Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas operasi rutin harian.

Peranan:	ICTSO, Pentadbir Sistem ICT

BIDANG A.9

A.9.1 Pengurusan Keselamatan Rangkaian *(Network Security Management)* 89
- A.9.1.1 Kawalan Rangkaian *(Network Controls)*
- A.9.1.2 Keselamatan Perkhidmatan Rangkaian *(Security of Network Services)*
- A.9.1.3 Pengasingan Rangkaian *(Segregation in Networks)*

A.9.2 Pemindahan Maklumat *(Information Transfer)* 91
- A.9.2.1 Polisi dan Prosedur Pemindahan Data dan Maklumat *(Information Transfer Policies and Procedures)*
- A.9.2.2 Perjanjian Mengenai Pemindahan Data dan Maklumat *(Agreements on Information Transfer)*
- A.9.2.3 Pengurusan Pesanan Elektronik *(Electronic Messaging Management)*
- A.9.2.4 Perjanjian Kerahsiaan atau Ketakdedahan *(Confidentiality Or Non-Disclosure Agreement)*

Keselamatan Komunikasi

Communications Security

A.9.1 PENGURUSAN KESELAMATAN RANGKAIAN

(NETWORK SECURITY MANAGEMANT)

Objektif: **Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.**

Kawalan:	Perkara:
A.9.1.1	**Kawalan Rangkaian** *(Network Controls)*

Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut:

(i) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi sistem rangkaian;

(ii) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir, gegaran dan habuk;

(iii) Peranti keselamatan seperti *firewall*, *Web Application Firewall* (WAF) dan *Intrusion Prevention System* (IPS) hendaklah dipasang mengikut kesesuaian keperluan;

(iv) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja;

(v) Sebarang keperluan penyambungan atau pemotongan rangkaian hendaklah melalui proses dan prosedur yang ditetapkan dan diselia pelaksanaannya;

(vi) Sebarang kerja pengubahsuaian, atau naik taraf peranti rangkaian perlulah mendapat kelulusan Pengurus ICT dan diselia oleh Pentadbir Rangkaian;

(vii) Semua pengguna hanya dibenarkan menggunakan fasiliti rangkaian sedia ada di MINDEF sahaja dan penggunaan peranti rangkaian luar seperti *switch*, *hub*, *access point* (AP) dan lain-lain perkakasan rangkaian tanpa kelulusan BPM adalah dilarang sama sekali;

(viii) Capaian pengguna jarak jauh *(remote user)* perlulah dikawal dan dipantau mengikut prosedur yang ditetapkan tertakluk kepada arahan dan polisi semasa Perkhidmatan;

(ix) Sebarang penggunaan perkhidmatan Internet mestilah menggunakan perkhidmatan rangkaian Internet rasmi yang disediakan MINDEF. Bagaimanapun, sebarang langganan talian Internet selain yang disediakan MINDEF akan dipertimbangkan tetapi tertakluk kepada kriteria berikut:

  (a) Terdapat keperluan kritikal dengan kelulusan khas pihak pengurusan tertinggi MINDEF; atau

  (b) Tiada liputan perkhidmatan Internet MINDEF di kawasan berkenaan; dan

  (c) PTJ mempunyai peruntukan bagi membiayai langganan khidmat Internet tersebut.

(x) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Agreement/ Assurance* (SLA) yang telah ditetapkan; dan

(xi) Semua perisian berkaitan rangkaian dan keselamatan seperti *sniffer*, *network analyser* atau perisian seperti *proxy avoidance* dan *unauthorized VPN software* adalah dilarang dipasang pada komputer pengguna atau sistem rangkaian MINDEF kecuali mendapat kebenaran ICTSO / Pengurus ICT.

Peranan:	ICTSO / Pengurus ICT / Pentadbir Sistem ICT / Pentadbir Rangkaian

Kawalan:	Perkara:
A.9.1.2	**Keselamatan Perkhidmatan Rangkaian** *(Security of Network Services)*

Perkhidmatan rangkaian hendaklah dipastikan sentiasa selamat serta dipantau bagi memastikan kerahsiaan, integriti dan ketersediaan maklumat terjamin.

Mekanisme keselamatan, tahap ketersediaan perkhidmatan dan keperluan pengurusan perkhidmatan rangkaian hendaklah dikenal pasti dan dinyatakan dalam perjanjian perkhidmatan rangkaian, sama ada perkhidmatan disediakan secara *in-house* ataupun *outsourced*.

Peranan:	ICTSO / Pentadbir Sistem ICT / Pentadbir Rangkaian / Pengguna

Kawalan:	Perkara:
A.9.1.3	**Pengasingan Rangkaian** *(Segregation in Networks)*

Pengasingan perkhidmatan rangkaian bertujuan meminimumkan risiko capaian tidak sah dan pengubahsuaian yang tidak dibenarkan.

Perkara–perkara yang perlu dipatuhi adalah:

(i) Melaksanakan konfigurasi hak capaian pengguna mengikut segmen rangkaian berdasarkan keperluan;

(ii) Menyediakan rangkaian terasing (*isolated network*) untuk orang luar atau pelawat yang hadir ke pejabat MINDEF dan memerlukan capaian Internet. Rangkaian ini hendaklah tidak dibenarkan mengakses rangkaian dalaman MINDEF dan perlu dipantau dari semasa ke semasa.

(iii) Mengemaskini hak capaian pengguna dari semasa ke semasa mengikut keperluan.

Peranan:	Pentadbir Sistem ICT / Pentadbir Rangkaian

A.9.2 PEMINDAHAN MAKLUMAT *(INFORMATION TRANSFER)*

Objektif: **Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.**

Kawalan:	Perkara:
A.9.2.1	**Polisi dan Prosedur Pemindahan Data dan Maklumat** *(Information Transfer Policies and Procedures)*

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:

(i) Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi;

(ii) Terma pemindahan data, maklumat dan perisian antara MINDEF dengan pihak luar hendaklah dimasukkan di dalam Perjanjian;

(iii) Media yang mengandungi maklumat perlu dilindungi;

(iv) Sebarang pemindahan maklumat di antara MINDEF dan agensi lain mestilah dikawal; dan

(v) Penggunaan perkhidmatan luar seperti aplikasi media sosial dan perkongsian fail untuk pemindahan maklumat rasmi Kerajaan perlu merujuk Arahan Keselamatan.

Peranan:	ICTSO / Pentadbir Sistem ICT / Pengguna

Kawalan:	Perkara:
A.9.2.2	**Perjanjian Mengenai Pemindahan Data dan Maklumat** *(Agreements on Information Transfer)*

MINDEF perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara MINDEF dengan pihak luar. Perkara yang perlu dipertimbangkan ialah:

(i) Penghantaran dan penerimaan maklumat MINDEF hendaklah dalam keadaan terkawal;

(ii) Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat MINDEF;

(iii) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan

(iv) MINDEF hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan mencegah ketirisan data.

Peranan:	CIO / ICTSO, Ketua Jabatan

Kawalan:	Perkara:
A.9.2.3	**Pengurusan Pesanan Elektronik** *(Electronic Messaging Management)*

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 Garis Panduan Penggunaan E-mel Kementerian Pertahanan.

Peranan:	Warga MINDEF

Kawalan:	Perkara:
A.9.2.4	**Perjanjian Kerahsiaan** *(Confidentiality Or Non-Disclosure Agreement)*

Syarat-syarat perjanjian kerahsiaan atau *Non-Disclosure Agreements* (NDA) perlu mengambil kira keperluan organisasi dan hendaklah disemak, dikemaskini dan didokumentasikan.

Pembekal / agensi luar hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat.

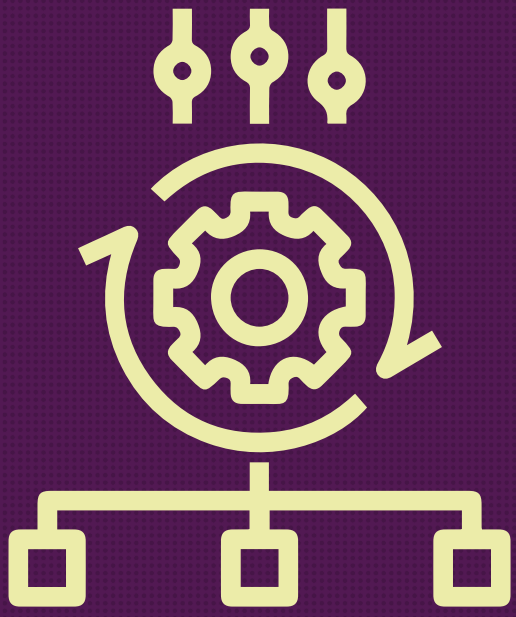
Peranan:	ICTSO / Pengurus ICT / Pentadbir Sistem ICT

BIDANG A.10

A.10.1 Keperluan Keselamatan Sistem Maklumat 95
(Security Requirements of Information Systems)
A.10.1.1 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat
(Information Security Requirements Analysis and Spesifications)
A.10.1.2 Melindungi Perkhidmatan Aplikasi Dalam Rangkaian Awam
(Securing Application Services on Public Networks)
A.10.1.3 Melindungi Transaksi Perkhidmatan Aplikasi
(Protecting Application Services Transaction)

A.10.2 Keselamatan Dalam Proses Pembangunan Dan Sokongan 97
(Security in Development and Support Services)
A.10.2.1 Polisi Keselamatan Dalam Pembangunan Sistem
(Security Policy In System Development)
A.10.2.2 Prosedur Kawalan Perubahan Sistem
(System Change Control Procedures)
A.10.2.3 Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi
(Technical Review Of Applications After Operating Platform Changes)
A.10.2.4 Prinsip Kejuruteraan Sistem Yang Selamat
(Secure System Engineering Principles)
A.10.2.5 Persekitaran Pembangunan Sistem Yang Selamat
(Secure Development Environment)
A.10.2.6 Pembangunan Sistem Secara Khidmat Sumber Luaran
(Outsourced Development)
A.10.2.7 Ujian Keselamatan Sistem *(System Security Testing)*
A.10.2.8 Pengujian Penerimaan Sistem *(System Acceptance Testing)*

A.10.3 Data Ujian *(Test Data)* 102
A.10.3.1 Perlindungan Data Ujian *(Protection of Test Data)*



Pemerolehan, Pembangunan Dan Penyenggaraan

System Acquisition, Development And Maintenance

A.10.1 KEPERLUAN KESELAMATAN SISTEM MAKLUMAT
(SECURITY REQUIREMENTS OF INFORMATION SYSTEMS)

Objektif: Memastikan keperluan keselamatan diambil kira dalam setiap fasa kitar hayat pembangunan sistem maklumat.

Kawalan:	Perkara:
A.10.1.1	**Analisis Keperluan dan Spesifikasi Keselamatan Maklumat** *(Information Security Requirements Analysis and Spesifications)*

Pembangunan sistem baharu atau penambahbaikan sistem sedia ada hendaklah mematuhi perkara-perkara berikut:

(i) Semua sistem yang dibangunkan sama ada secara dalaman atau khidmat luaran hendaklah dikaji supaya mengikut keperluan pengguna dan selaras dengan dasar atau peraturan semasa yang berkuat kuasa;

(ii) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang ditetapkan; dan

(iii) Ujian keselamatan hendaklah dilakukan di setiap peringkat pembangunan sistem bagi memastikan integriti data.

Peranan:	Pentadbir Sistem ICT, Pembekal

Kawalan:	Perkara:
A.10.1.2	**Melindungi Perkhidmatan Aplikasi Dalam Rangkaian Awam** *(Securing Application Services on Public Networks)*

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:

(i) Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala;

(ii) Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala;

(iii) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan MFA *(Multi Factor Authentication)*;

(iv) Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi;

(v) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan

(vi) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.

Peranan:	Pengurus ICT, Pentadbir Sistem ICT, Pembekal

Kawalan:	Perkara:
A.10.1.3	**Melindungi Transaksi Perkhidmatan Aplikasi** *(Protecting Application Services Transaction)*

Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulang tayang mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi;

(ii) Memastikan semua aspek transaksi dipatuhi:

  (a) Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan;

  (b) Mengekalkan kerahsiaan maklumat;

  (c) Mengekalkan privasi pihak yang terlibat; dan

  (d) Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi.

(iii) Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh Kerajaan.

Peranan:	Pengurus ICT, Pentadbir Sistem ICT

A.10.2 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN

(SECURITY IN DEVELOPMENT AND SUPPORT SERVICES)

Objektif: **Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan siber yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.**

Kawalan:	Perkara:
A.10.2.1	**Polisi Keselamatan Dalam Pembangunan Sistem** *(Security Policy In System Development)*

Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi.

Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Keselamatan persekitaran pembangunan;

(ii) Keselamatan pangkalan data;

(iii) Keperluan keselamatan dalam fasa reka bentuk;

(iv) Keperluan *check point* keselamatan dalam carta perbatuan projek;

(v) Keperluan pengetahuan ke atas keselamatan aplikasi;

(vi) Keselamatan dalam kawalan versi; dan

(vii) Bagi pembangunan melalui khidmat sumber luaran *(outsource)*, pembekal yang dilantik hendaklah berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.

Peranan:	ICTSO / Pengurus ICT / Pentadbir Sistem ICT

Kawalan:	Perkara:
A.10.2.2	**Polisi Keselamatan Dalam Pembangunan Sistem** *(Security Policy In System Development)*

Prosedur kawalan perubahan sistem hendaklah diwujudkan bagi mengawal sebarang perubahan ke atas sistem maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(i) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, didokumenkan dan disahkan sebelum diguna pakai;

(ii) Setiap aplikasi perlu dikaji semula dan diuji apabila terdapat perubahan/naiktaraf sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor;

(iii) Kawalan perlu dibuat terhadap sebarang perubahan ke atas sistem aplikasi atau pakej perisian bagi memastikan ianya terhad mengikut keperluan sahaja; dan

(iv) Capaian kepada kod sumber *(source code)* aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.

Peranan:	Pengurus ICT

Kawalan:	Perkara:
A.10.2.3	**Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi** *(Technical Review Of Applications After Operating Platform Changes)*

Sebarang cadangan perubahan platform hendaklah berasaskan kepada kajian teknikal bagi memastikan pengoperasian sistem tidak terjejas. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(i) Memastikan sistem aplikasi dan integriti data disemak supaya operasi sistem tidak terjejas apabila perubahan *platform* dilakukan;

(ii) Perubahan *platform* dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan

(iii) Sebarang perubahan hendaklah selari dengan Pelan Kesinambungan Perkhidmatan MINDEF.

Peranan:	Pentadbir Sistem ICT

Kawalan:	Perkara:
A.10.2.4	**Prinsip Kejuruteraan Sistem Yang Selamat** *(Secure System Engineering Principles)*

Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, di selenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat.

Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat.

Semua peringkat pembangunan sistem hendaklah mengambil kira prinsip kejuruteraan sistem berikut:

(i) Asas Keselamatan *(Security Foundation)*

Merujuk kepada PKS MINDEF dan pekeliling semasa yang berkuat kuasa dalam reka bentuk sesuatu sistem.

(ii) Berasaskan Risiko *(Risk Based)*

Mengurangkan risiko ke tahap boleh terima.

(iii) Mudah Diguna *(Ease of Use)*

Mempunyai ciri-ciri open standard untuk portability dan interoperability.

(iv) Meningkatkan Daya Tahan *(Increase Resilience)*

Memastikan tiada sebarang kelemahan melalui pelaksanaan keselamatan *(layered security)*.

(v) Mengurang Kelemahan *(Reduce Vulnerabilities)*

Meminimumkan kelemahan disebabkan reka bentuk yang kompleks supaya penyenggaraan sistem mudah dilaksanakan.

(vi) 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.

Peranan:	Pentadbir Sistem ICT

Kawalan:	Perkara:
A.10.2.5	**Persekitaran Pembangunan Sistem Yang Selamat** *(Secure Development Environment)*

Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem.

Adalah perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira:

(i) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem;

(ii) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran;

(iii) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem;

(iv) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem;

(v) Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan

(vi) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.

Peranan:	Pentadbir Sistem ICT

Kawalan:	Perkara:
A.10.2.6	**Pembangunan Sistem Secara Khidmat Sumber Luaran** *(Outsourced Development)*

Pembangunan sistem secara khidmat sumber luaran perlu dikawal selia dan dipantau. *Intellectual Property Rights* (IPR) dan kod sumber *(source code)* hendaklah menjadi hak milik Kerajaan.

Semasa fasa pembangunan sistem oleh pihak tersebut, kod sumber *(source code)* yang dibangunkan perlu diakses dan disemak oleh MINDEF.

Peranan:	Pengurus ICT / Pentadbir Sistem ICT

Kawalan:	Perkara:
A.10.2.7	**Ujian Keselamatan Sistem** *(System Security Testing)*

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:

(i) Merancang dan melaksanakan penilaian risiko mengikut keperluan bagi mengenal pasti dan melaksana kawalan yang sesuai bagi pengesahan dan perlindungan integriti data dalam aplikasi;

(ii) Merancang dan melaksana ujian keselamatan yang bersesuaian mengikut fasa di dalam kitar hayat pembangunan sistem *(Software Development Life Cycle atau SDLC)* bagi mengenal pasti kelemahan sistem; dan

(iii) Membuat semakan pengesahan sistem aplikasi untuk mengenal pasti sebarang pencemaran maklumat sama ada disebabkan oleh kesilapan atau disengajakan.

Peranan:	Pentadbir Sistem ICT

Kawalan:	Perkara:
A.10.2.8	**Pengujian Penerimaan Sistem** *(System Acceptance Testing)*

Program Pengujian Penerimaan Sistem (Ujian Penerimaan Pengguna dan Ujian Penerimaan Akhir) hendaklah dilaksanakan berdasarkan kriteria yang telah ditetapkan sebelum sistem diguna pakai.

Amalan pengujian mestilah menurut standard yang semasa serta menepati amalan terbaik dalam industri.

Peranan:	Pentadbir Sistem ICT, Pengguna, Pembekal

A.10.3 DATA UJIAN *(TEST DATA)*

Objektif: Untuk memastikan perlindungan ke atas data yang digunakan untuk pengujian.

Kawalan:	Perkara:
A.10.3.1	**Perlindungan Data Ujian** *(Protection of Test Data)*

Data ujian hendaklah disediakan dengan secukupnya sebelum ujian dilaksanakan.
Kaedah menjana data ujian adalah seperti berikut:

(i) Menyediakan secara manual;

(ii) Salin data daripada persekitaran produksi *(production)* kepada persekitaran pengujian;

(iii) Salin data ujian daripada sistem aplikasi terdahulu *(legacy)*;

(iv) Menyediakan secara automatik seperti *web service* atau sebarang *tools* yang menjana data; atau

(v) *Back-end Data Injection*.

Perkara–perkara yang perlu dipatuhi adalah:

(i) Sebarang prosedur kawalan persekitaran produksi *(production environment)* hendaklah juga dilaksanakan dalam persekitaran pengujian;

(ii) Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian;

(iii) Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan

(iv) Mengaktifkan audit log bagi merekodkan semua aktiviti pengujian dan pengemaskinian untuk tujuan statistik, pemulihan, keselamatan dan pengesahan data.

Peranan:	Pentadbir Sistem ICT, Pengguna

BIDANG A.11

A.11.1 Keselamatan Maklumat Dalam Hubungan Pembekal 105
(Information Security in Supplier Relationships)
A.11.1.1 Polisi Keselamatan Maklumat Untuk Hubungan Pembekal
(Information Security Policy for Supplier Relationships)
A.11.1.2 Kawalan Keselamatan Maklumat Melalui Perjanjian Dengan Pembekal
(Addressing Information Security Within Supplier Agreements)
A.11.1.3 Rantaian Bekalan Produk ICT
(Information and Communication Technology Supply Chain)

A.11.2 Pengurusan Penyampaian Perkhidmatan Pembekal 108
(Supplier Service Delivery Management)
A.11.2.1 Pemantauan dan Kajian Perkhidmatan Pembekal
(Monitoring and Review Supplier Services)
A.11.2.2 Pengurusan Perubahan Perkhidmatan Pembekal
(Managing Changes to Supplier Services)

Hubungan Dengan Pembekal

Supplier Relationship

A.11.1 KESELAMATAN MAKLUMAT DALAM HUBUNGAN PEMBEKAL

(INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS)

Objektif: Memastikan aset ICT MINDEF yang boleh diakses pembekal dilindungi.

Kawalan:	Perkara:
A.11.1.1	**Polisi Keselamatan Maklumat Untuk Hubungan Pembekal** *(Information Security Policy for Supplier Relationships)*

Semua syarikat pembekal adalah tertakluk kepada Dasar Keselamatan Kerajaan yang berkuat kuasa. Perkara–perkara yang perlu dipatuhi adalah seperti berikut:

(i) Syarikat pembekal hendaklah menandatangani **Surat Akuan Pematuhan Polisi Keselamatan Siber Kementerian Pertahanan seperti di Lampiran A** ;

(ii) Syarikat pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas; dan

(iii) Akses syarikat pembekal ke atas aset ICT MINDEF hendaklah sentiasa dikawal dan dipantau.

Peranan:	Pengurus ICT, Syarikat Pembekal

Kawalan:	Perkara:
A.11.1.2	**Kawalan Keselamatan Maklumat Melalui Perjanjian Dengan Pembekal** *(Addressing Information Security Within Supplier Agreements)*

Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi. Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak MINDEF selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa.

Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut:

i) MINDEF hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan;

ii) Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan;

iii) Semua wakil syarikat pembekal hendaklah melepasi tapisan keselamatan daripada agensi berkaitan;

iv) Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi;

v) Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal;

vi) Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut:

   a) Badan penilai pihak ketiga adalah bebas dan berintegriti;

   b) Badan penilai pihak ketiga adalah kompeten;

   c) Kriteria penilaian;

   d) Parameter pengujian; dan

   e) Andaian yang dibuat berkaitan dengan skop penilaian.

vii) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan MINDEF; dan

viii) Syarikat pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh MINDEF.

Peranan:	Syarikat Pembekal

Kawalan:	Perkara:
A.11.1.3	**Rantaian Bekalan Produk ICT** *(Information and Communication Technology Supply Chain)*

Perjanjian dengan syarikat pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut:

(i) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan;

(ii) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk;

(iii) Memastikan jaminan daripada syarikat pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik; dan

(iv) Pembekal utama hendaklah memastikan produk atau perkhidmatan yang diberikan adalah selamat daripada unsur-unsur yang boleh mengganggu kelancaran perkhidmatan ICT di MINDEF.

Peranan:	Syarikat Pembekal

A.11.2 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PEMBEKAL *(SUPPLIER SERVICE DELIVERY MANAGEMENT)*

Objektif: Untuk mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal.

Kawalan:	Perkara:
A.11.2.1	**Pemantauan dan Kajian Perkhidmatan Pembekal** *(Monitoring and Review Supplier Services)*

Prestasi perkhidmatan pembekal hendaklah sentiasa dipantau, diaudit dan dikaji semula secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut:

(i) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan;

(ii) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan

(iii) Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.

Peranan:	Pemilik projek

Kawalan:	Perkara:
A.11.2.2	**Pengurusan Perubahan Perkhidmatan Pembekal** *(Managing Changes to Supplier Services)*

Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan, dengan mengambil kira kepentingan maklumat, sistem dan proses perniagaan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti yang berikut:

(i) Perubahan dalam perjanjian dengan pembekal;

(ii) Perubahan yang dilakukan oleh MINDEF bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan

(iii) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baharu, produk-produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.

Peranan:	Pengurus ICT / Pemilik Projek / Pembekal

BIDANG A.12

A.12.1 Pengurusan Insiden Keselamatan Maklumat dan Penambahbaikan 111
(Management of Information Security Incidents and Improvements)
A.12.1.1 Tanggungjawab dan Prosedur *(Responsibilities and Procedures)*
A.12.1.2 Pelaporan Kejadian Keselamatan Maklumat
(Reporting Information Security Events)
A.12.1.3 Pelaporan Kelemahan Keselamatan Maklumat
(Reporting Security Weakness)
A.12.1.4 Penilaian dan Keputusan Mengenai Kejadian Keselamatan Maklumat
(Assessment and Decision on Information Security Events)
A.12.1.5 Tindak Balas Terhadap Insiden Keselamatan Maklumat
(Response to Information Security Incidents)
A.12.1.6 Pembelajaran Daripada Insiden Keselamatan Maklumat
(Learning from Information Security Incidents)
A.12.1.7 Pengumpulan Bahan Bukti *(Collection of Evidence)*

Pengurusan Insiden Keselamatan ICT

ICT Security Incident Management

A.12.1 PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT DAN PENAMBAHBAIKAN

(MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENT)

Objektif: **Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi tentang kejadian dan kerentanan keselamatan.**

Kawalan:	Perkara:
A.12.1.1	**Tanggungjawab dan Prosedur** *(Responsibilities and Procedures)*

Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan insiden MINDEF adalah berpandukan Prosedur Operasi Standard (SOP) Pengendalian Insiden Keselamatan ICT MINDEF. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(i) Memberikan kesedaran berkaitan Prosedur Operasi Standard Pengendalian Insiden Keselamatan ICT MINDEF dan hebahan kepada warga MINDEF sekiranya ada perubahan; dan

(ii) Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.

Peranan:	ICTSO, MINDEFCERT

Kawalan:	Perkara:
A.12.1.2	**Pelaporan Kejadian Keselamatan Maklumat** *(Reporting Information Security Events)*

Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada MINDEFCERT yang kemudiannya perlu melaporkan kepada ICTSO dengan kadar segera. Insiden keselamatan ICT adalah meliputi perkara-perkara berikut:

(i) Maklumat didapati atau disyaki hilang (serangan virus, kecurian dan lain-lain);

(ii) Maklumat didedahkan kepada pihak yang tidak diberi kuasa;

(iii) Sistem maklumat disyaki digunakan tanpa kebenaran;

(iv) Kecurian data dan maklumat;

(v) Mekanisme kawalan akses seperti kata laluan dikompromi;

(vi) Sistem beroperasi secara tidak normal seperti kehilangan maklumat, kegagalan fungsi sistem atau ralat dalam komunikasi data; dan

(vii) Berlaku pencerobohan dan penyelewengan data.

Peranan:	ICTSO, Pengurus ICT, MINDEFCERT

Kawalan:	Perkara:
A.12.1.3	**Pelaporan Kelemahan Keselamatan Maklumat** *(Reporting Security Weakness)*

Warga MINDEF dan pembekal yang menggunakan sistem dan perkhidmatan maklumat MINDEF dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT.

Peranan:	Warga MINDEF, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital MINDEF

Kawalan:	Perkara:
A.12.1.4	**Penilaian dan Keputusan Mengenai Kejadian Keselamatan Maklumat** *(Assessment and Decision on Information Security Events)*

Sebarang insiden hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.

Peranan:	ICTSO, MINDEFCERT

Kawalan:	Perkara:
A.12.1.5	**Tindak Balas Terhadap Insiden Keselamatan Maklumat** *(Response to Information Security Incidents)*

Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CERT.

Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut:

(i) Menghubungi pihak yang terlibat dengan secepat mungkin;

(ii) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku;

(iii) Menjalankan kajian forensik sekiranya perlu;

(iv) Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti;

(v) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;

(vi) Menyediakan pelan kontigensi dan mengaktifkan Pelan Kesinambungan Perkhidmatan sekiranya perlu;

(vii) Melaksanakan pengasingan ke atas capaian rangkaian sekiranya perlu;

(viii) Menyediakan tindakan pemulihan segera; dan

(ix) Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.

Peranan:	ICTSO, MINDEFCERT

Kawalan:	Perkara:
A.12.1.6	**Pembelajaran Daripada Insiden Keselamatan Maklumat** *(Learning from Information Security Incidents)*

Pengetahuan yang diperoleh daripada penganalisaan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya.

Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah.

Peranan:	ICTSO, MINDEFCERT

Kawalan:	Perkara:
A.12.1.7	**Pengumpulan Bahan Bukti** *(Collection of Evidence)*

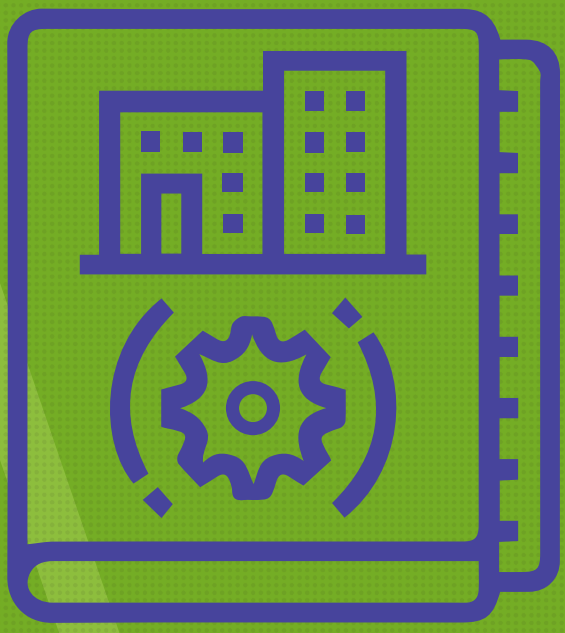
Proses pengutipan, pengumpulan dan penganalisaan bahan bukti mengikut arahan dan prosedur-prosedur semasa yang telah ditetapkan untuk tujuan rekod serta penyampaian bahan bukti.

Peranan:	ICTSO, MINDEFCERT

BIDANG A.13

A.13.1 Kesinambungan Keselamatan Maklumat *(Information Security Continuity)* 117
A.13.1.1 Perancangan Kesinambungan Keselamatan Maklumat *(Planning Information Security Continuity)*
A.13.1.2 Pelaksanaan Kesinambungan Keselamatan Maklumat *(Implementing Information Security Continuity)*
A.13.1.3 Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat *(Verify, Review and Evaluate Information Security Continuity)*

A.13.2 Lewahan *(Redundancy)* 119
A.13.2.1 Ketersediaan Kemudahan Pemprosesan Maklumat *(Availability of Information Process Facilities)*



Pengurusan Kesinambungan Perkhidmatan

Business Continuity Management

A.13.1 KESINAMBUNGAN KESELAMATAN MAKLUMAT

(INFORMATION SECURITY CONTINUITY)

Objektif: Kesinambungan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan perkhidmatan di MINDEF.

Kawalan:	Perkara:
A.13.1.1	**Perancangan Kesinambungan Keselamatan Maklumat** *(Planning Information Security Continuity)*

Keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi MINDEF.

MINDEF juga perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP) MINDEF;

(ii) Menetapkan polisi PKP;

(iii) Mengenal pasti perkhidmatan kritikal;

(iv) Melaksanakan Kajian Impak Perkhidmatan *(Business Impact Analysis)* dan Penilaian Risiko terhadap perkhidmatan kritikal;

(v) Membangunkan Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak Balas Kecemasan dan Pelan Pemulihan Bencana ICT;

(vi) Melaksanakan program kesedaran dan latihan pasukan PKP dan warga MINDEF;

(vii) Melaksanakan simulasi ke atas pelan di para (v);

(viii) Melaksanakan penyelenggaraan ke atas pelan di para (v); dan

(ix) Memastikan dokumen di para (v) sentiasa dikemaskini dan ditambahbaik.

Peranan:	Koordinator PKP / Pasukan Tindak Balas Kecemasan / Pasukan Komunikasi Krisis / Pasukan Pemulihan Bencana ICT

Kawalan:	Perkara:
A.13.1.2	**Pelaksanaan Kesinambungan Keselamatan Maklumat** *(Implementing Information Security Continuity)*

MINDEF hendaklah menyediakan, mendokumenkan, melaksanakan dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan.

Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

(i) Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal MINDEF yang telah dikenal pasti berdasarkan kepada Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT terkini;

(ii) Melaksanakan *post-mortem* dan mengemaskini pelan-pelan PKP;

(iii) Mengemas kini pelan-pelan PKP jika berlaku perubahan kepada fungsi kritikal MINDEF;

(iv) Mengemas kini struktur tadbir urus PKP MINDEF jika berlaku pertukaran pegawai bersara dan bertukar keluar; dan

(v) Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP.

Peranan:	Koordinator PKP / Pasukan Tindak Balas Kecemasan / Pasukan Komunikasi Krisis / Pasukan Pemulihan Bencana ICT

Kawalan:	Perkara:
A.13.1.3	**Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat** *(Verify, Review and Evaluate Information Security Continuity)*

MINDEF hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.

Peranan:	Pengurusan Atasan MINDEF, Koordinator PKP / Pasukan Tindak Balas Kecemasan / Pasukan Komunikasi Krisis, Pasukan Pemulihan Bencana ICT / Pemilik Perkhidmatan Kritikal MINDEF dalam PKP / warga MINDEF

A.13.2 LEWAHAN *(REDUNDANCY)*

Objektif: **Untuk memastikan ketersediaan kemudahan pemprosesan maklumat dengan mewujudkan lewahan.**

Kawalan:	Perkara:
A.13.2.1	**Ketersediaan Kemudahan Pemprosesan Maklumat** *(Availability of Information Process Facilities)*

Kemudahan pemprosesan maklumat MINDEF perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji *(failover test)* keberkesanannya dari semasa ke semasa.

Peranan:	Pengurus ICT / Pentadbir Sistem ICT

BIDANG A.14

A.14.1 Pematuhan terhadap Keperluan Perundangan dan Kontrak 123
(Compliance with Legal and Contractual Requirements)
A.14.1.1 Pengenalpastian Keperluan Undang-Undang dan Kontrak Yang Terpakai
(Identification of Applicable Legislation and Contractual Agreement)
A.14.1.2 Hak Harta Intelek *(Intellectual Property Rights)*
A.14.1.3 Perlindungan Rekod *(Protection of Records)*
A.14.1.4 Privasi dan Perlindungan Maklumat Peribadi
(Privacy and Protection of Personally Identifiable Information)
A.14.1.5 Peraturan Kawalan Kriptografi
(Regulation of Cryptographic Controls)

A.14.2 Kajian Semula Keselamatan Maklumat *(Information Security Reviews)* 125
A.14.2.1 Kajian Semula Keselamatan Maklumat Secara Berkecuali
(Independent Review of Information Security)
A.14.2.2 Pematuhan Polisi dan Piawaian Keselamatan
(Compliance with Security Policies and Standards)
A.14.2.3 Kajian Semula Pematuhan Teknikal *(Technical Compliance Review)*

Pematuhan

Compliance

A.14.1 PEMATUHAN TERHADAP KEPERLUAN PERUNDAGAN KONTRAK

(COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS)

Objektif: Mempertingkatkan keupayaan tahap keselamatan siber bagi mengelak dari pelanggaran mana-mana undang-undang, kewajiban berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.

Kawalan:	Perkara:
A.14.1.1	**Pengenalpastian Keperluan Undang-Undang dan Kontrak Yang Terpakai** *(Identification of Applicable Legislation and Contractual Agreement)*

Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga MINDEF, pembekal, pakar runding dan pihak yang mengakses dan menggunakan perkhidmatan digital MINDEF. Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dirujuk oleh semua pengguna di MINDEF dan pembekal adalah seperti di **LAMPIRAN B.**

Peranan:	Warga MINDEF, pembekal, pakar runding dan pihak yang mengakses dan menggunakan perkhidmatan digital MINDEF

Kawalan:	Perkara:
A.14.1.2	**Hak Harta Intelek** *(Intellectual Property Rights)*

Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual.

Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.

Peranan:	Warga MINDEF, pembekal, pakar runding dan pihak yang mengakses dan menggunakan perkhidmatan digital MINDEF dan ATM

Kawalan:	Perkara:
A.14.1.3	**Perlindungan Rekod** *(Protection of Records)*

Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.

Peranan:	Warga MINDEF, pembekal, pakar runding dan pihak yang mengakses dan menggunakan perkhidmatan digital MINDEF

Kawalan:	Perkara:
A.14.1.4	**Privasi dan Perlindungan Maklumat Peribadi** *(Privacy and Protection of Personally Identifiable Information)*

MINDEF hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.

Peranan:	Warga MINDEF, pembekal, pakar runding dan pihak yang mengakses dan menggunakan perkhidmatan digital MINDEF

Kawalan:	Perkara:
A.14.1.5	**Peraturan Kawalan Kriptografi** *(Regulation of Cryptographic Controls)*

Kawalan kriptografi hendaklah dilaksanakan berdasarkan kepada perjanjian kontrak, undang-undang dan peraturan-peraturan berkaitan.

Peranan:	Warga MINDEF, pembekal, pakar runding dan pihak yang mengakses dan menggunakan perkhidmatan digital MINDEF

A.14.2 KAJIAN SEMULA KESELAMATAN MAKLUMAT

(INFORMATION SECURITY REVIEWS)

Objektif: Untuk memastikan keselamatan maklumat dan keselamatan siber dilaksanakan semakan dan pindaan sebagai penambahbaikan berterusan mengikut polisi dan prosedur MINDEF.

Kawalan:	Perkara:
A.14.2.1	**Kajian Semula Keselamatan Maklumat Secara Berkecuali** *(Independent Review of Information Security)*

Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.

Peranan:	ICTSO

Kawalan:	Perkara:
A.14.2.2	**Pematuhan Polisi dan Piawaian Keselamatan** *(Compliance with Security Policies and Standards)*

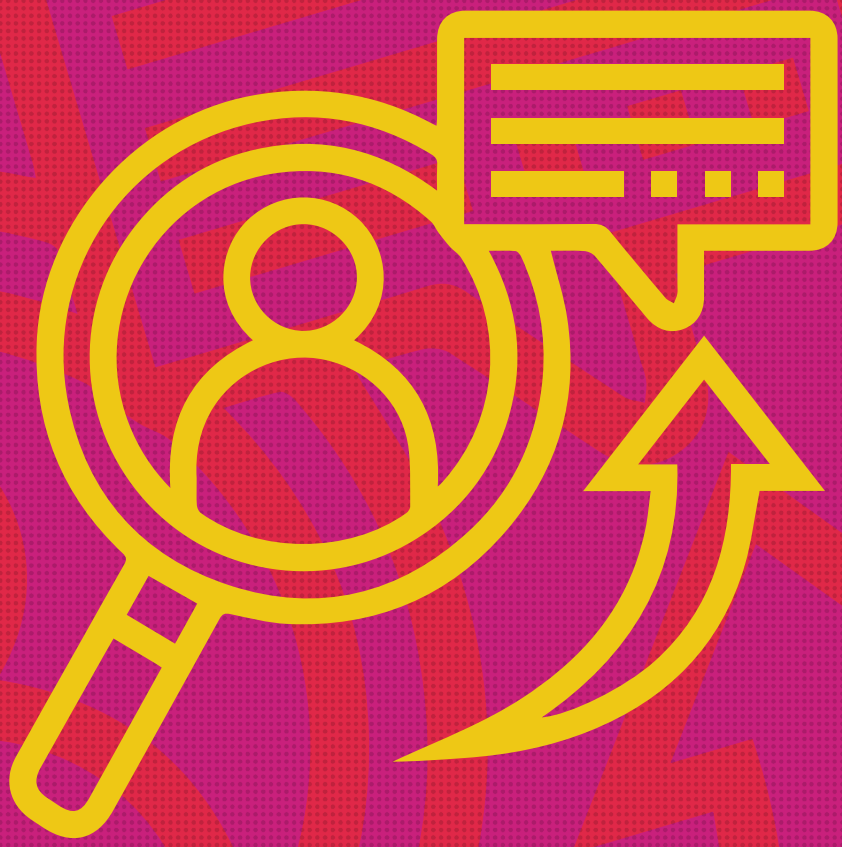
MINDEF hendaklah melaksanakan kajian semula secara berkala terhadap pematuhan prosedur pemprosesan maklumat supaya selaras dengan polisi, piawaian dan keperluan teknikal berkaitan keselamatan.

Peranan:	ICTSO

Kawalan:	Perkara:
A.14.2.3	**Kajian Semula Pematuhan Teknikal** *(Technical Compliance Review)*

MINDEF hendaklah melaksanakan kajian semula pematuhan teknikal sistem-sistem maklumat secara berkala terhadap semua polisi dan piawaian teknikal yang telah ditetapkan.

Peranan:	ICTSO



Lampiran

Reference

LAMPIRAN A

SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER KEMENTERIAN PERTAHANAN

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 Polisi Keselamatan Siber Kementerian Pertahanan Malaysia (PKS MINDEF).
2. Sekiranya saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan undang-undang boleh diambil ke atas diri saya.

.....
(Tandatangan)

Tarikh: .....

.....
Tandatangan Pegawai Keselamatan ICT (ICTSO)

Cop Jabatan

Tarikh: .....

RUJUKAN

Polisi Keselamatan Siber Kementerian Pertahanan (PKS MINDEF) ini hendaklah dibaca bersama dengan akta, warta kerajaan, pekeliling, surat pekeliling, dan peraturan yang berkaitan dan sedang berkuatkuasa seperti berikut:

1. Akta Arkib Negara 2003
2. Akta Angkatan Tentera 1972
3. Akta Rahsia Rasmi 1972
4. Akta Jenayah Komputer 1997
5. Akta Tandatangan Digital 1997
6. Akta Komunikasi dan Multimedia 1998
7. Akta Aktiviti Kerajaan Elektronik 2007
8. Arahan Keselamatan (Semakan dan Pindaan 2017)
9. Arahan Teknologi Maklumat 2007
10. Arahan No. 24 Majlis Keselamatan Negara Dasar & Mekanisme Pengurusan Krisis Siber Negara
11. Arahan No. 26 Majlis Keselamatan Negara Pengurusan Keselamatan Siber Negara
12. Garis Panduan Penggunaan E-Mel Kementerian Pertahanan versi 1.0 Tahun 2021
13. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan bertarikh 1 Oktober 2000
14. Surat Arahan Ketua Setiausaha Negara Penamaan Ketua Pegawai Maklumat Sektor Awam Tahun 2000
15. *Malaysian Public Sector Management of Information & Communications Technology Security Handbook* (MyMIS) bertarikh 15 Jan 2002
16. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 Nov 2005
17. Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 - Panduan Pengurusan Pejabat
18. Surat Pekeliling Am Bilangan 3 Tahun 2009 - Garis Panduan Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam bertarikh 17 Nov 2009
19. Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam bertarikh 24 Nov 2010
20. Surat Arahan Ketua Pengarah MAMPU - Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 dalam Sektor Awam bertarikh 24 Nov 2010

21. Surat Arahan Ketua Pengarah MAMPU - Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam bertarikh 22 Jan 2010

22. Surat Arahan Ketua Pengarah MAMPU - Amalan Terbaik Penggunaan Media Jaringan Sosial di Sektor Awam bertarikh 8 April 2011

23. Perintah Am Angkatan Tentera Bil 1/13. Arahan Keselamatan Maklumat – Perintah Pencegahan Pencemaran Maklumat ATM melalui Platform Siber bertarikh 11 Januari 2013

24. Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan Risiko Keselamatan Maklumat Menggunakan MyRAM App 2.0 di Agensi Sektor Awam bertarikh 12 Ogos 2015

25. Pekeliling Kemajuan Pentadbiran Awam Bilangan 3 Tahun 2015 Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [*Government Public Key Infrastructure* (GPKI)] bertarikh 23 Oktober 2015

26. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) versi 1.0 bertarikh 1 April 2016

27. Perintah Am Angkatan Tentera Bil 1/2017. Garis Panduan Keselamatan Teknologi Komunikasi dan Maklumat (ICT) Angkatan Tentera Malaysia bertarikh 8 Februari 2017

28. Perintah Am Angkatan Tentera Bil 2/2017. Garis Panduan Keselamatan Komunikasi dan Elektronik (KESKOM) Angkatan Tentera Malaysia bertarikh 8 Februari 2017

29. Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian *Government Computer Emergency Response Team* (GCERT) oleh NACSA bertarikh 28 Januari 2019

30. Surat Pemakluman Pengurusan Maklumat Pegawai Keselamatan ICT (ICTSO) Sektor Awam bertarikh 28 Februari 2019

31. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021 Dasar Perkhidmatan Komputeran Awan Sektor Awam bertarikh 10 Jun 2021

32. Surat Pekeliling Am Bilangan 2 Tahun 2021 Garis Panduan Pengurusan Keselamatan Maklumat melalui Pengkomputeran Awan *(Cloud Computing)* dalam Perkhidmatan Awam bertarikh 9 Ogos 2021

33. Pekeliling Kemajuan Pentadbiran Awam Bil 2 Tahun 2021 Dasar Perkongsian Data Sektor Awam 27 Ogos 2021

34. Surat Pekeliling Am Bil 4 Tahun 2022 Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022

KEMENTERIAN PERTAHANAN
BAHAGIAN PENGURUSAN MAKLUMAT

ISBN 978-967-26651-1-3

9 7 8 9 6 7 2 6 6 5 1 1 3