

# TENTERA UDARA DI RAJA MALAYSIA



## MANUAL PENGURUSAN KESELAMATAN ICT TUDM

(Publikasi ini PU 9110 2<sup>nd</sup> Edition Manual Pengurusan Keselamatan ICT TUDM  
07 Apr 2014 adalah bagi menggantikan (*Supersedes*) PU 9110 1<sup>st</sup> Edition  
Dasar Pengurusan Keselamatan ICT TUDM Dated 03 Sep 2008  
Rujuk penaja: MTU/BTMK/204/2 bertarikh 18 Feb 14.)

# PENGESAHAN PENERIMAAN PUBLIKASI / PERLAKSANAAN PINDAAN/ KAJI SELIDIK PELANGGAN

(Dikembalikan ke PUSPEKA (UP: TDC) dalam masa 14 hari dari tarikh penghantaran diterima)

KEPADA

PUSAT PERKHIDMATAN KEJURUTERAAN AEROSPACE (PUSPEKA)  
d/a PANGKALAN UDARA SUBANG  
40000 SHAH ALAM  
SELANGOR DARUL EHSAN

RUJUKAN TDC

PUSPEKA/KEJ/580/1 BERTARIKH 30 DIS 2014

NO PROJEK/ID  
(JIKA ADA)

JMS 526/14 – BERTARIKH 19 DIS 2014 - CETAK DAN AGIHAN

Dilengkapkan oleh pihak TDC

## A. BUTIR-BUTIR DOKUMEN / PUBLIKASI

A1 NO. PUBLIKASI : PU 9110 2<sup>ND</sup> EDITION

A2 TAJUK : MANUAL KESELAMATAN ICT TUDM.

Hendaklah dilengkapkan oleh penerima dokumen

## B. BUTIR-BUTIR PENERIMAAN

B1 NO. TEN/PKT/NAMA :  
B2 UNIT / SKUADRON :  
B3 SEKSYEN :  
B4 NO TEL : Samb. :  
B5 TARIKH TERIMA :

ADALAH DISAHKAN BAHAWA PADA TARIKH YANG DINYATAKAN DIATAS, PUBLIKASI YANG TERLIBAT TELAH  
DITERIMA DAN DIREKODKAN DENGAN SEWAJARNYA MENGIKUT ARAHAN/POLISI SEMASA.

B6

TANDATANGAN

B7

Cop Pasukan

Hendaklah dilengkapkan oleh pelaksana pindaan

## C. BUTIR-BUTIR PERLAKSANAAN / PENGESAHAN PINDAAN

C1 NO. TEN/PANGKAT / NAMA :  
C2 NO. TEL :  
C3 NO / TARIKH PINDAAN TERDAHULU :  
C4 TARIKH PERLAKSANAAN PINDAAN  
TERKINI :  
C5 JUMLAH PUBLIKASI TERLIBAT : KTI PUB. NO. SALINAN PUB.

ADALAH DISAHKAN BAHAWA PADA TARIKH YANG DINYATAKAN DIATAS, SEMUA PINDAAN KEATAS PUBLIKASI YANG  
TERLIBAT TELAH DILAKSANAKAN DAN DIREKODKAN DENGAN SEWAJARNYA MENGIKUT ARAHAN/POLISI SEMASA.

C6

TANDATANGAN

Panduan mengisi disertakan di bahagian belakang borang.

C7

Cop Pasukan

## D1. BORANG KAJI SELIDIK KEPUASAN PELANGGAN

Apakah pandangan anda terhadap perkhidmatan dan kerja yang telah dilaksanakan oleh  
bahagian ini?

|   |                     | * |
|---|---------------------|---|
| 1 | PERLU DI PERBAIKI   |   |
| 2 | KURANG MEMUASKAN    |   |
| 3 | SEDERHANA           |   |
| 4 | BERPUAS HATI        |   |
| 5 | SANGAT BERPUAS HATI |   |

\* (Sila √ kotak di sebelah)



SALINAN NO: 03 .....

# TENTERA UDARA DI RAJA MALAYSIA



## MANUAL PENGURUSAN KESELAMATAN ICT TUDM

1. MAKLUMAT YANG TERKANDUNG DALAM DOKUMEN INI TIDAK BOLEH DIBERITAHU SECARA LANGSUNG ATAU TIDAK LANGSUNG KEPADA AKHBAR ATAU SESIAPA YANG TIDAK BERHAK MENERIMANYA. DOKUMEN INI ADALAH HAKMILIK KERAJAAN MALAYSIA DAN DIMAKSUDKAN BAGI MAKLUMAN ORANG-ORANG YANG PERLU MENGETAHUI KANDUNGAN DALAMNYA DALAM MASA MENJALANKAN TUGAS-TUGAS RASMI MEREKA.
2. Penamaan dan penomboran baru Publikasi TUDM telah dipersetujui melalui Mesyuarat Jawatankuasa Penasihat Panglima Tentera Udara JPPTU Siri 104/2005. Sementara Mesyuarat 'Senior Engineers Forum' (SEF) 1/106 pula telah mengesahkan penggunaanya sebagai dokumen yang sah (Legal Documents) di seluruh TUDM kandungan, risalah dan kembaran akan dibuat secara berperingkat.
3. Sesiapa yang menjumpai dokumen ini adalah dikehendaki oleh Undang-undang menyerahkannya kepada pejabat Daerah, Balai Polis atau Pejabat Angkatan Tentera untuk dihantar kepada Bahagian Staf Perisikan Pertahanan (BSPP) berserta dengan keterangan-keterangan termasuk tarikh, masa, tempat dan bagaimana dijumpai. Menyimpan dan membina dokumen ini dengan tiada kebenaran adalah suatu kesalahan di bawah AKTA RAHSIA RASMI 1972.

**MANUAL PENGURUSAN KESELAMATAN ICT TUDM****PENDAHULUAN**

1. Publikasi Udara (PU) 9110 pada asalnya merupakan Dasar Keselamatan ICT (DKICT) TUDM. Namun, dalam mesyuarat Jawatankuasa ICT (JKICT TUDM) Siri 1/13 yang dilaksanakan pada 20 Nov 13 telah mengambil keputusan untuk menukarnya kepada Manual Keselamatan ICT (MKICT) TUDM sesuai dengan perubahan yang telah dilakukan pada DKICT TUDM bagi menepati perkembangan teknologi semasa dalam TUDM.
2. Manual Pengurusan Keselamatan ICT TUDM adalah dokumen yang digunakan sebagai garis panduan yang perlu dipatuhi oleh setiap warga TUDM untuk menjamin keselamatan ICT TUDM.
3. Dokumen ini tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Manual ini hendaklah dibaca bersama dokumen-dokumen mengenai piawaian, garis panduan, prosedur dan langkah keselamatan ICT TUDM yang akan dikeluarkan dari semasa ke semasa.
4. Publikasi ini PU 9110 2<sup>nd</sup> Edition Manual Pengurusan Keselamatan ICT TUDM 07 Apr 2014 adalah bagi menggantikan (*Supersedes*) PU 9110 1<sup>st</sup> Edition Dasar Pengurusan Keselamatan ICT TUDM Dated 03 Sep 2008 Rujuk penaja: MTU/BTMK/204/2 bertarikh 18 Feb 14.
5. Sebarang maklum balas atau perubahan berkaitan dengan manual ini hendaklah dimajukan ke alamat berikut:

**Markas Tentera Udara**  
**(Bahagian Teknologi Maklumat dan Komunikasi)**  
**Aras 6, Bangunan TH Selborn**  
**153 Jalan Tun Razak**  
**50400 KUALA LUMPUR**  
**(Untuk Perhatian: Pengarah)**

Telefon: 03-26873001  
Faks : 03-26873093  
E-mel : [btmk.tudm@mod.gov.my](mailto:btmk.tudm@mod.gov.my)

07 April 2014

  
TAN SRI DATO' SRI RODZALI BIN DAUD  
Jen TUDM  
Panglima Tentera Udara



## SENARAI MUKASURAT YANG TERBABIT

[illegible]

iii  
TERHAD

## MANUAL PENGURUSAN KESELAMATAN ICT TUDM

REKOD PINDAAN

| Senarai Pindaan |        | **Dipinda Oleh:<br>No, Pangkat dan Nama | Tandatangan | Tarikh |
|-----------------|--------|-----------------------------------------|-------------|--------|
| *No.            | Tarikh |                                         |             |        |
| 1               |        |                                         |             |        |
| 2               |        |                                         |             |        |
| 3               |        |                                         |             |        |
| 4               |        |                                         |             |        |
| 5               |        |                                         |             |        |
| 6               |        |                                         |             |        |
| 7               |        |                                         |             |        |
| 8               |        |                                         |             |        |
| 9               |        |                                         |             |        |
| 10              |        |                                         |             |        |
| 11              |        |                                         |             |        |
| 12              |        |                                         |             |        |
| 13              |        |                                         |             |        |
| 14              |        |                                         |             |        |
| 15              |        |                                         |             |        |
| 16              |        |                                         |             |        |
| 17              |        |                                         |             |        |
| 18              |        |                                         |             |        |
| 19              |        |                                         |             |        |
| 20              |        |                                         |             |        |
| 21              |        |                                         |             |        |
| 22              |        |                                         |             |        |
| 23              |        |                                         |             |        |
| 24              |        |                                         |             |        |

**NOTA:** \* No. Pindaan ini membabitkan pindaan ke atas muka surat kepada risalah yang dinyatakan di muka surat iii (senarai muka surat terbabit)

\*\* Pindaan hanya boleh dibuat oleh anggota Perpustakaan Teknikal atau pemilik manual ini sahaja.



**MANUAL PENGURUSAN KESELAMATAN ICT TUDM****ISI KANDUNGAN**

| <b>No Siri</b> | <b>Tajuk</b>                           | <b>Muka Surat</b> |
|----------------|----------------------------------------|-------------------|
| 1.             | Muka Surat Tajuk                       | i                 |
| 2.             | Pendahuluan                            | ii                |
| 3.             | Senarai Muka Surat Yang Terbabit       | iii               |
| 4.             | Rekod Pindaan                          | iv                |
| 5.             | Isi Kandungan                          | v                 |
| 6.             | Petunjuk Kepada Muka Surat             | vi                |
| 7.             | Senarai Agihan                         | vii               |
| 8.             | Singkatan/Terminologi- (Abbreviations) | viii              |
| 9.             | <b>BAHAGIAN : 1</b>                    | 1.1               |
| 10.            | <b>BAHAGIAN : 2</b>                    | 2.1               |
| 11.            | <b>BAHAGIAN : 3</b>                    | 3.1               |
| 12.            | <b>BAHAGIAN : 4</b>                    | 4.1               |
| 13.            | <b>BAHAGIAN : 5</b>                    | 5.1               |
| 14.            | <b>BAHAGIAN : 6</b>                    | 6.1               |

**MANUAL PENGURUSAN KESELAMATAN ICT TUDM****PETUNJUK KEPADA MUKA SURAT**

| No Siri | Tajuk                                                                  | Muka Surat                      |
|---------|------------------------------------------------------------------------|---------------------------------|
| 1.      | Muka Surat Tajuk                                                       | i                               |
| 2.      | Pendahuluan                                                            | ii                              |
| 3.      | Senarai Muka Surat Yang Terbabit                                       | iii                             |
| 4.      | Rekod Pindaan                                                          | iv                              |
| 5.      | Isi Kandungan                                                          | v                               |
| 6.      | Petunjuk Kepada Muka Surat                                             | vi                              |
| 7.      | Senarai Agihan                                                         | vii – 1 drp 2                   |
| 8.      | Singkatan/Terminologi- (Abbreviations)                                 | viii – 1 drp 11                 |
| 9.      | <b>BAHAGIAN :1</b>                                                     | 1.1                             |
|         | RISALAH : 1 PERNYATAAN DAN PERLAKSANAAN                                | 1.1 – 1 drp 2                   |
|         | RISALAH : 2 PERNYATAAN KESELAMATAN ICT TUDM                            | 1.2 – 1 drp 9                   |
|         | RISALAH : 3 PELAKSANAAN MANUAL KESELAMATAN ICT TUDM                    | 1.3 – 1 drp 2                   |
| 10.     | <b>BAHAGIAN :2</b>                                                     | 2.1                             |
|         | RISALAH : 1 PENGURUSAN KESELAMATAN ICT TUDM                            | 2.1 – 1 drp 9                   |
|         | RISALAH : 2 PENGURUSAN ASET                                            | 2.2 – 1 drp 4                   |
|         | RISALAH : 3 KESELAMATAN PERSONEL                                       | 2.3 – 1 drp 4                   |
|         | RISALAH : 4 KESELAMATAN FIZIKAL DAN PERSEKITARAN                       | 2.4 – 1 drp 12                  |
| 11.     | <b>BAHAGIAN :3</b>                                                     | 3.1                             |
|         | RISALAH : 1 PENGURUSAN OPERASI DAN KOMUNIKASI                          | 3.1 – 1 drp 13                  |
|         | RISALAH : 2 KAWALAN CAPAIAN                                            | 3.2 – 1 drp 9                   |
|         | RISALAH : 3 PEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM            | 3.3 – 1 drp 4                   |
|         | RISALAH : 4 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT KEMBARAN A | 3.4 – 1 drp 5<br>3.4A – 1 drp 2 |
|         | RISALAH : 5 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN                      | 3.5 – 1 drp 4                   |
|         | RISALAH: 6 PEMATUHAN                                                   | 3.6 – 1 drp 4                   |



## MANUAL PENGURUSAN KESELAMATAN ICT TUDM

SENARAI AGIHAN

| UNIT                                       | SEKSYEN                                   | KUANTITI | NO SALINAN |
|--------------------------------------------|-------------------------------------------|----------|------------|
| Markas Tentera Udara                       | Pejabat PTU                               | 1        | 01         |
|                                            | BTMK                                      | 2        | 02 - 03    |
|                                            | Perpustakaan Teknikal MTU                 | 2        | 04 - 05    |
|                                            |                                           |          |            |
| Markas Pemerintahan Operasi Udara          | Pejabat Panglima                          | 1        | 06         |
|                                            | Perpustakaan Teknikal MOU                 | 1        | 07         |
|                                            |                                           |          |            |
| Markas Wilayah Udara 1                     | Pejabat Panglima                          | 1        | 08         |
|                                            | Perpustakaan Teknikal 1 Div               | 1        | 09         |
|                                            |                                           |          |            |
| Markas Wilayah Udara 2                     | Pejabat Panglima                          | 1        | 10         |
|                                            | Perpustakaan Teknikal 2 Div               | 1        | 11         |
|                                            |                                           |          |            |
| Markas Pemerintahan Bantuan Udara          | Pejabat Panglima                          | 1        | 12         |
|                                            | Perpustakaan Teknikal MLU                 | 1        | 13         |
|                                            |                                           |          |            |
| Markas Pendidikan dan Latihan Udara (MPLU) | Pejabat Panglima                          | 1        | 14         |
|                                            | Perpustakaan Teknikal MPLU                | 1        | 15         |
|                                            |                                           |          |            |
| Pangkalan Udara Butterworth                | Komander Pangkalan                        | 1        | 16         |
|                                            | Perpustakaan Teknikal Cawang Kejuruteraan | 1        | 17         |
|                                            |                                           |          |            |
| Pangkalan Udara Kuantan                    | Komander Pangkalan                        | 1        | 18         |
|                                            | Perpustakaan Teknikal Cawang Kejuruteraan | 1        | 19         |
|                                            |                                           |          |            |
| Pangkalan Udara Subang                     | Komander Pangkalan                        | 1        | 20         |
|                                            | Perpustakaan Teknikal Cawang Kejuruteraan | 1        | 21         |
|                                            |                                           |          |            |
| Pangkalan Udara KL                         | Komander Pangkalan                        | 1        | 22         |
|                                            | Perpustakaan Teknikal Cawang Kejuruteraan | 1        | 23         |
|                                            |                                           |          |            |
| Pangkalan Udara Gong Kedak                 | Komander Pangkalan                        | 1        | 24         |
|                                            | Perpustakaan Teknikal Cawang Kejuruteraan | 1        | 25         |
|                                            |                                           |          |            |
| Pangkalan Udara Kuching                    | Komander Pangkalan                        | 1        | 26         |
|                                            | Perpustakaan Teknikal Cawang Kejuruteraan | 1        | 27         |
|                                            |                                           |          |            |
| Pangkalan Udara Labuan                     | Komander Pangkalan                        | 1        | 28         |
|                                            | Perpustakaan Teknikal Cawang Kejuruteraan | 1        | 29         |
|                                            |                                           |          |            |
| Kolej Tentera Udara                        | Komandan                                  | 1        | 30         |
|                                            | Perpustakaan Teknikal Cawang Kejuruteraan | 1        | 31         |
|                                            |                                           |          |            |
| Markas Rejimen TUDM                        | Pegawai Memerintah                        | 1        | 32         |
|                                            | Perpustakaan Rejimen TUDM                 | 1        | 33         |
|                                            |                                           |          |            |

| UNIT                  | SEKSYEN                           | KUANTITI | NO SALINAN |
|-----------------------|-----------------------------------|----------|------------|
| ILTU                  | Komandan                          | 1        | 34         |
|                       | Perpustakaan Teknikal ILTU        | 1        | 35         |
|                       |                                   |          |            |
| SITU                  | Pegawai Memerintah                | 1        | 36         |
|                       | Perpustakaan Teknikal SITU        | 1        | 37         |
|                       |                                   |          |            |
| TUDM Bukit Ibam       | Pegawai Memerintah Skn 322        | 1        | 38         |
|                       | Perpustakaan Teknikal Skn 322     | 1        | 39         |
|                       |                                   |          |            |
| TUDM Bukit Luncu      | Pegawai Memerintah Skn 323        | 1        | 40         |
|                       | Perpustakaan Teknikal Skn 323     | 1        | 41         |
|                       |                                   |          |            |
| TUDM Bukit Kubong     | Pegawai Memerintah Skn 340        | 1        | 42         |
|                       | Perpustakaan Teknikal Skn 340     | 1        | 43         |
|                       |                                   |          |            |
| TUDM Kinrara          | Pegawai Memerintah PLPL           | 1        | 44         |
|                       | Perpustakaan Teknikal PLPL        | 1        | 45         |
|                       |                                   |          |            |
| PUKALUB Subang        | Pegawai Memerintah                | 1        | 46         |
|                       | Perpustakaan Teknikal PUKALUB Sub | 1        | 47         |
|                       |                                   |          |            |
| PUKALUB Kota Kinabalu | Pegawai Memerintah                | 1        | 48         |
|                       | Perpustakaan Teknikal PUKALUB KK  | 1        | 49         |
|                       |                                   |          |            |
| PUSPEKA               | BPPT (TDC)                        | 2        | 50 - 51    |



## MANUAL PENGURUSAN KESELAMATAN ICT TUDM

SINGKATAN/TERMINOLOGI - (ABBREVIATIONS)

| Singkatan/Terminologi       | Nama Penuh/Makna                                                                                                                                                                                                                                                                                         |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Agensi Pusat                | Agensi yang bertanggungjawab membantu, menyelaras dan mengawal perjalanan agensi-agensi mengurus seperti menggubal dan membentuk dasar dan perancangan sesuatu organisasi.                                                                                                                               |
| Akauntabiliti               | <ol style="list-style-type: none"> <li>1. Kepertanggungjawab (Kamus Istilah Pentadbiran Perniagaan Pengajian Tinggi – DBP)</li> <li>2. Bertanggungjawab kepada seseorang mengenai sesuatu (Kamus Dwi Bahasa - DBP)</li> <li>3. Bertanggungjawab , Boleh diharapkan (Dunia Baru Webster Kamus)</li> </ol> |
| Akses                       | Proses memasuki ruang simpanan untuk menyimpan atau mendapatkan data kembali.                                                                                                                                                                                                                            |
| Arahan Keselamatan Kerajaan | Panduan mengenai peraturan-peraturan keselamatan yang perlu dipatuhi oleh semua kakitangan kerajaan.                                                                                                                                                                                                     |
| Aset ICT TUDM               | Komponen-komponen yang terdiri daripada perkakasan, perisian dan sistem rangkaian ICT.                                                                                                                                                                                                                   |
| Jejak Audit                 | Satu proses untuk mengenalpasti semua aktiviti yang dilakukan oleh komputer dalam memproses kemasukan data, penjaan <i>output</i> dan segala aktiviti yang terlibat di antaranya.                                                                                                                        |
| Autentikasi                 | Satu proses mengenalpasti semua aktiviti yang dilakukan oleh komputer dalam memproses kemasukan data, penjaan <i>output</i> dan segala aktiviti yang terlibat di antaranya.                                                                                                                              |
| BTMK                        | Bahagian Teknologi Maklumat & Komunikasi                                                                                                                                                                                                                                                                 |
| <i>Backbone</i> rangkaian   | Mekanisme sambungan primer dari jaringan terdistribusi berstruktur hirarki. Dapat dipastikan bahawa semua sistem yang memiliki sambungan ke sebuah sistem lanjutan pada jaringan <i>backbone</i> , juga memiliki sambungan ke jaringan lainnya.                                                          |
| <i>Backup</i>               | Membuat salinan data supaya salinan tambahan ini mungkin akan digunakan sekiranya berlaku kehilangan data.                                                                                                                                                                                               |

**Singkatan/Terminologi****Nama Penuh/Makna**

Bahagian Staf Perisikan  
Pertahanan (BSPP)

Bahagian Staf Perisikan Pertahanan (BSPP) adalah satu jabatan/agensi yang mengendalikan tugas-tugas perisikan kepada ATM. Bahagian ini bertanggungjawab secara terus kepada Kementerian Pertahanan melalui pejabat Panglima Angkatan Tentera.

*Business Continuity Planning* (BCP)

Pelan tindakan untuk merancang aktiviti-aktiviti bisnes.

*Central Processing Unit* (CPU)

Unit Pemprosesan Utama iaitu yang mengandungi *processor*, *hard disk*, RAM dan *motherboard*.

CHIEF INFORMATION  
OFFICER (CIO)

Individu yang dilantik dan bertanggungjawab dalam menguruskan keselamatan maklumat di sesebuah agensi kerajaan.

*Computer Emergency  
Response Team* (CERT)

Satu agensi yang akan bertindak sekiranya berlaku bencana atau perkara-perkara yang tidak diingini.

*Clear Desk* dan *Clear Screen*

Tidak meninggalkan bahan-bahan sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.

*Capability Maturity Model* (CMM)

Kaedah yang diguna pakai bagi menghasilkan dan menghalusi proses pembangunan perisian sebuah organisasi. Model ini menggambarkan lima tahap yang bersifat evolusi terancang, proses-proses yang lebih matang dan sistematik.

*Cracker*

Individu atau kumpulan yang cuba untuk memasuki sesuatu rangkaian komputer dan sekaligus memusnahkan atau mengubah sistem yang telah direkabentuk bagi tujuan mencuri maklumat atau merosakkan sistem komputer.

*Corrective Maintenance*

Pembaikan yang dibuat terhadap perkakasan dan perisian apabila berlaku kerosakan.

Data

1. Sebutan umum bagi unsur maklumat seperti fakta, nombor, huruf, atau lambang yang dapat diproses atau dihasilkan oleh komputer.
2. Bacaan yang dihasilkan oleh pengukuran atau pengujian.
3. Maklumat kod berangka yang tersusun.

*Data Packet*

*Packet* adalah unit asas bagi komunikasi dalam rangkaian.

Enkripsi

Proses di mana data disusun ke dalam satu bentuk yang sukar dibaca atau tidak dapat difahami untuk kerahsiaan transmisi atau tujuan keselamatan lain.



**Singkatan/Terminologi****Nama Penuh/Makna***Emergency Response Team (ERT)*

Pasukan yang bertanggungjawab untuk memberi perhatian terhadap ancaman kritikal dengan tahap bahaya melebihi tahap jangkaan yang normal.

*Firewall*

Sebuah program sekuriti sistem kombinasi daripada perkakasan & perisian yang mengawal had pendedahan komputer atau rangkaian komputer daripada diserang penceroboh (*hacker* dan *cracker*); kebiasannya digunakan pada sambungan rangkaian setempat (LAN) dengan internet.

*Fire Drill*

Satu kaedah yang dipraktikan bagi proses pemindahan dalam sesebuah bangunan sekiranya berlaku kebakaran atau desakan-desakan lain.

*Government Computer Emergency Response (GCERT )*

Merupakan satu pasukan khas yang terletak di MAMPU bertanggungjawab untuk mengendalikan semua insiden yang dilaporkan

*Hub*

Peralatan rangkaian menghubungkan satu stesen kerja dengan stesen kerja yang lain.

*Integriti*

1. Merujuk pada kamus Oxford, Integriti merujuk pada mutu serta kualiti dalam bersikap jujur dan telus.
2. Kamus English Collin pula menakrifkan integriti adalah seumpama anutan terhadap prinsip-prinsip akhlak, kejujuran, kebersatuan dan kebaikan. Maklumat/data hendaklah tepat, lengkap dan hanya boleh diubah dengan cara yang dibenarkan.

*Intrusion Detection Sistem (IDS)*

Satu peralatan yang digunakan untuk memantau atau merekod cubaan pencerobohan.

*Internet*

Sistem perangkaian antarabangsa yang membolehkan pengguna mencapai maklumat pangkalan data dari seluruh dunia.

*Information Security*

Proses dan mekanisme untuk melindungi maklumat.

*Insiden keselamatan ICT*

Bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat.

*ISDN (Integrated Sistem Digital Network)*

Talian digital yang digunakan untuk mencapai internet.

**Singkatan/Terminologi****Nama Penuh/Makna**

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jawatankuasa Pemandu ICT MinDef                | Jawatankuasa Tertinggi di peringkat Kementerian Pertahanan yang diketuai oleh CIO dan dianggotai oleh semua Ketua-ketua Jabatan ICT di setiap perkhidmatan. Jawatankuasa ini berperanan menetapkan dasar ICT MinDef.                                                                                                                                                                                                                                              |
| Jabatan                                        | Formasi, Pasukan, Bahagian atau Cawangan.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Jawatankuasa Teknikal ICT MinDef               | Jawatankuasa yang dibentuk bagi membuat penilaian dari aspek keupayaan teknikal dan keselamatan bagi sesuatu projek ICT.                                                                                                                                                                                                                                                                                                                                          |
| Kata laluan                                    | Kata yang terdiri daripada gabungan huruf dan/atau nombor yang membentuk kod unik. Kata ini perlu dimaklumkan kepada sistem sebelum pengguna dibolehkan menggunakan sumber sistem. Kaedah ini melindungi sistem daripada digunakan oleh orang yang tidak mempunyai kebenaran penggunaan.                                                                                                                                                                          |
| Kawalan Akses                                  | Pengawasan terhadap pencapaian untuk perkakasan, perisian dan rangkaian.                                                                                                                                                                                                                                                                                                                                                                                          |
| Kawalan Persekitaran                           | <ol style="list-style-type: none"> <li>1. Set peraturan tertentu yang menunjukkan cara bagaimana data boleh diwakili.</li> <li>2. Peraturan dan resam yang menentukan bagaimana isyarat yang mewakili data boleh dibentuk, dihantar, diterima, dan diproses dalam suatu sistem perhubungan.</li> <li>3. Bentuk berlambang yang mewakili data atau suruhan atur cara komputer atau mikropemproses yang boleh diterima dan diproses oleh mesin tersebut.</li> </ol> |
| Kerajaan Elektronik<br>( <i>E-Government</i> ) | Sistem pengurusan secara elektronik untuk melancarkan tugas-tugas pentadbiran dalam kerajaan.                                                                                                                                                                                                                                                                                                                                                                     |
| Keselamatan Fizikal                            | Faktor-faktor keselamatan luaran yang perlu diambil kira untuk menjamin keselamatan perkakasan dan perisian.                                                                                                                                                                                                                                                                                                                                                      |
| Keselamatan Personel                           | Persekitaran yang disediakan bagi menjamin keselamatan staf.                                                                                                                                                                                                                                                                                                                                                                                                      |
| Ketua Jabatan                                  | Pegawai tentera atau awam yang mengetuai sesebuah unit/pangkalan/kapal dan jabatan awam.                                                                                                                                                                                                                                                                                                                                                                          |



| Singkatan/Terminologi                                                                | Nama Penuh/Makna                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kriptografi                                                                          | Secara umum adalah ilmu atau seni menjaga kerahsiaan maklumat. Kaedah untuk menukar maklumat biasa kepada format yang tidak boleh difahami bagi menjaga dari aspek keselamatan, kerahsiaan, keabsahan, autentikasi dan integriti data.                                                                         |
| LAN ( <i>Local Area Network</i> )                                                    | Singkatan bagi <i>Local Area Network</i> . Rangkaian komputer yang dihadkan untuk menyambungkan komputer dan peranti persisian yang berada dalam suatu kawasan kecil yang sama, seperti bilik, tapak, atau bangunan kecil.                                                                                     |
| <i>Leased Line</i>                                                                   | Talian suwa yang telah disewa secara tetap oleh Kementerian.                                                                                                                                                                                                                                                   |
| <i>Lightning Arrestor</i>                                                            | Peralatan yang digunakan bagi melindungi perkakasan elektrik dari terkena kilat.                                                                                                                                                                                                                               |
| MAC ( <i>Media Access Control</i> )                                                  | Merujuk kepada kawalan akses perantaraan alat rangkaian komputer.                                                                                                                                                                                                                                              |
| MAFSI ( <i>Malaysian Armed Forces Security Instruction</i> )                         | Arahan keselamatan digunapakai oleh semua perkhidmatan ATM dan anggota awam di dalam Kementerian Pertahanan.                                                                                                                                                                                                   |
| <i>Mail server</i>                                                                   | Pelayan yang digunakan sebagai platform oleh sesebuah organisasi untuk menguruskan penerimaan dan penghantaran e-mel.                                                                                                                                                                                          |
| MAMPU ( <i>Malaysian Administrative Modernisation and Management Planning Unit</i> ) | Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, adalah badan pentadbiran utama di Malaysia yang berfungsi sebagai pusat bagi pemodenan tadbiran dan perancangan tenaga manusia.                                                                                                                   |
| Maklumat Berdarjah                                                                   | Maklumat rasmi yang telah diklasifikasikan mengikut klasifikasi rahsia besar, rahsia, sulit dan terhad. Maklumat ini boleh didapati dalam bentuk percetakan atau pun dalam bentuk digital.                                                                                                                     |
| Media Storan                                                                         | Peralatan untuk menyimpan maklumat digital.                                                                                                                                                                                                                                                                    |
| <i>Malicious Code</i>                                                                | Kod <i>Malicious</i> (juga dipanggil pelaku musnah - <i>vandals</i> ) adalah satu ancaman baru Internet yang tidak boleh dikawal dengan berkesan oleh perisian antivirus konvensional. Berbeza dengan virus-virus yang memerlukan seorang pengguna untuk melaksanakan sebuah program dengan tujuan menyebabkan |

**Singkatan/Terminologi****Nama Penuh/Makna**

|                                                  |                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                  | kerosakan, <i>vandals</i> adalah aplikasi yang boleh dilaksanakan secara auto. Virus-virus dan <i>worms</i> boleh diklasifikasikan sebahagian daripada <i>malicious code</i> , kekeliruan sering berlaku untuk membezakannya kerana kedua-duanya berkongsi matlamat utama iaitu pereplikaan ( <i>replication</i> ). |
| Modem                                            | Satu peranti yang berfungsi menghubungkan komputer dengan internet.                                                                                                                                                                                                                                                 |
| Pegawai Keselamatan ICT(ICTSO)                   | Pegawai yang bertanggungjawab untuk menjaga keselamatan maklumat ICT.                                                                                                                                                                                                                                               |
| Pegawai Keselamatan Kerajaan                     | Bertanggungjawab menasihati, membantu, menjalankan pemeriksaan dan penyiasatan keselamatan di semua jabatan secara bebas.                                                                                                                                                                                           |
| Pelan Strategik MinDef                           | Pelan strategik 5 tahun bagi menjalankan projek-projek ICT.                                                                                                                                                                                                                                                         |
| Pelayan ( <i>Server</i> )                        | Pelayan ( <i>Server</i> ) adalah satu aplikasi atau alat yang menyediakan perkhidmatan untuk menghubungkan <i>client</i> sebagai sebahagian daripada seni bina pelayan-pelanggan ( <i>client-server</i> ).                                                                                                          |
| Pelan Pemulihan Bencana                          | Perancangan sebuah organisasi menangani sebarang bencana yang berpotensi berlaku.                                                                                                                                                                                                                                   |
| Pengodam ( <i>hacker</i> )                       | Individu atau kumpulan yang berhasrat untuk mencapai maklumat atau sistem rangkaian walaupun mereka tidak berhak untuk berbuat demikian.                                                                                                                                                                            |
| Pengguna MinDef                                  | Tentera dan penjawat awam, yang bekerja dan menggunakan rangkaian ICT di mana-mana organisasi di bawah Kementerian Pertahanan.                                                                                                                                                                                      |
| Pentadbir Sistem ( <i>System Administrator</i> ) | Pegawai yang bertanggungjawab untuk menjalankan tugas-tugas pentadbiran sesuatu sistem.                                                                                                                                                                                                                             |
| Perisian                                         | Bahagian sistem komputer yang berfungsi menjalankan sistem, dan terdiri daripada cara, rutin, subrutin, dan suruhan yang ditulis dalam bahasa pengaturcaraan.                                                                                                                                                       |
| Perkakasan                                       | Komponen fizikal atau peralatan yang membentuk sistem komputer.                                                                                                                                                                                                                                                     |
| Pihak Ketiga                                     | Juru Perunding atau Kontraktor.                                                                                                                                                                                                                                                                                     |
| <i>Power Over-Rating</i>                         | Kuasa elektrik yang melebihi had.                                                                                                                                                                                                                                                                                   |



**Singkatan/Terminologi****Nama Penuh/Makna**

|                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rangkaian Dalam ( <i>Private Network</i> )                    | Rangkaian komputer persendirian yang digunakan bagi sesuatu projek atau perkhidmatan.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Rangkaian Awam ( <i>Public Network</i> )                      | Rangkaian komputer awam yang digunakan secara bersama oleh semua perkhidmatan tentera dan awam untuk mengakses Internet.                                                                                                                                                                                                                                                                                                                                                                                   |
| Rangkaian Selamat ( <i>Secured Network</i> )                  | Rangkaian komputer strategik yang memproses maklumat berdarjah keselamatan yang tinggi seperti P4x, AMSS dan SIS.                                                                                                                                                                                                                                                                                                                                                                                          |
| <i>Preventive Maintenance</i>                                 | Penyelenggaraan pencegahan berjadual untuk melindungi perkakasan, perisian atau sistem operasi.                                                                                                                                                                                                                                                                                                                                                                                                            |
| RADIUS ( <i>Remote Authentication Dial-In User Services</i> ) | Sejenis peralatan rangkaian yang digunakan untuk menghubungkan antara satu rangkaian dengan rangkaian lain. Satu keselamatan protokol pengesahan berdasarkan <i>clients</i> dan <i>server</i> yang mana digunakan dengan luas oleh penyedia perkhidmatan internet (ISP – <i>Internet Service Provider</i> ) yang bukan daripada <i>server Microsoft</i> . RADIUS adalah cara yang paling terkenal bagi mengesahkan ketulenan dan memberi kuasa dailan ( <i>dial-up</i> ) bagi pengguna rangkaian hari ini. |
| Rahsia                                                        | Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing.                                                                                                                                                                                                                                                   |
| Rahsia Besar                                                  | Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia.                                                                                                                                                                                                                                                                                                                                                             |
| Rangkaian Mindef                                              | Semua rangkaian yang wujud di bawah Kementerian Pertahanan.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <i>Restore</i>                                                | Mengembalikan bentuk asalnya agar dapat digunakan dan berfungsi seperti sediakala.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <i>Risk Assesment</i>                                         | Analisa risiko untuk mengenalpasti kelemahan-kelemahan yang terdapat dalam sistem yang boleh memberi ancaman kepada keselamatan sistem.                                                                                                                                                                                                                                                                                                                                                                    |
| <i>Router</i>                                                 | Sejenis peralatan rangkaian yang digunakan untuk menghubungkan antara satu rangkaian dengan rangkaian lain.                                                                                                                                                                                                                                                                                                                                                                                                |

**Singkatan/Terminologi****Nama Penuh/Makna***Scanning Tool*

Sebarang jenis utiliti dalam bentuk perisian atau perkakasan yang berupaya untuk melakukan pengimbasan terhadap sistem rangkaian.

*Screen saver*

Adalah sejenis aturcara komputer yang direka untuk mencegah "Tindihan putih Phosphor" (*Phosphor burn-in*) di *monitor* komputer dengan pengisian imej-imej atau corak-corak yang menarik apabila komputer tidak digunakan.

*Secondary Storage*

Storan sekunder yang berfungsi untuk menyokong storan utama.

*Secured Network*

Sistem Rangkaian terselamat di mana maklumat yang melaluinya dienkripi.

*Smartcard*

Kad Pintar yang mempunyai cip untuk menyimpan maklumat secara digital.

*SSID (Service Set Identifier)*

SSID adalah nama bagi rangkaian kawasan tempatan tanpa wayar (*wireless*) WLAN. Semua alat tanpa wayar (*wireless*) WLAN mesti menggunakan SSID yang serupa dan teratur untuk berkomunikasi di antara satu sama lain.

*Stakeholder*

Merupakan orang terpenting dalam sesebuah projek. Terdiri daripada pengguna-pengguna akhir atau pelanggan-pelanggan. Bertanggungjawab dalam mempengaruhi rekabentuk dan orang yang akan memperolehi faedah apabila projek siap.

*Stesen Kerja*

Komputer peribadi yang telah disambungkan secara rangkaian dan digunakan oleh pengguna untuk mengakses sistem aplikasi.

*Sistem Teknologi Maklumat*

Sistem yang berkaitan dengan pengumpulan, pemasukan, penyimpanan, pemprosesan, pengeluaran, dan penyebaran maklumat.

*Sulit*

Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.



**Singkatan/Terminologi****Nama Penuh/Makna**

Tandatangan Digital  
(*Digital Signature*)

Tandatangan digital adalah kod digital yang dapat diselitkan pada pesanan/mesej yang dikirim secara elektronik. Tanda tangan inilah yang menjadi identifikasi si pengirim. Sama seperti tanda tangan tertulis, tujuan tanda tangan digital adalah untuk menjamin serta mengesahkan bahawa pengirim pesanan/mesej itu adalah daripada orang yang sah.

Teknologi Maklumat dan Komunikasi  
(ICT)

Sebarang bentuk teknologi berasaskan elektronik yang merangkumi pengkomputeran dan telekomunikasi yang digunakan untuk menguruskan maklumat secara keseluruhan.

*Telecommuting*

Merupakan satu cara yang membolehkan pegawai untuk melaksanakan tugas di mana sahaja dan dalam masa yang sama berhubung secara terus (Online) dengan pejabat.

*Telnet*

Satu Protokol yang akan membenarkan stesen kerja untuk memasuki persekitaran UNIX dengan menggunakan sesi terminal (*terminal session*).

Terhad

Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakan juga diberi satu tahap perlindungan keselamatan.

UPS (*Uninterruptable Power Supply*)

Peranti yang mengandungi bateri yang menyimpan kuasa yang bertujuan untuk mengambil alih peranan kuasa elektrik sekiranya berlaku gangguan bekalan kuasa.

VADS

VADS Berhad (VADS) adalah salah sebuah syarikat penyedia perkhidmatan ICT terulung di Malaysia. Usaha sama antara IBM Global Network Services dan Telekom Malaysia Berhad.

Virus

Atur cara komputer yang disorok di dalam atur cara lain dan dapat menyalin dirinya sendiri ke dalam perisian lain apabila atur cara itu digunakan.

VPN (*Virtual Private Network*)

Rangkaian Maya Persendirian yang menggunakan infrastruktur telekomunikasi awam, tetapi masih mengekalkan pemilikan (*privacy*) melalui protokol tertentu dan lain-lain prosedur keselamatan.

WAN (*Wide Area Network*)

Rangkaian komputer untuk menyambungkan komputer dan peranti perisian yang terletak jauh di antara satu sama lain. Rangkaian kawasan luas memerlukan penggunaan modem.

**Singkatan/Terminologi****Nama Penuh/Makna**

Warga KEMENTAH

Merujuk kepada semua pegawai dan kakitangan Kementerian Pertahanan termasuk awam dan tentera.

*Web Server*

Pelayan yang digunakan sebagai platform oleh sesebuah organisasi untuk meletakkan aplikasi web yang dilancarkan ke Internet.

*Wire Tapping*

Adalah pengawasan terhadap perbualan telefon dan akses Internet yang dilakukan oleh pihak ketiga.

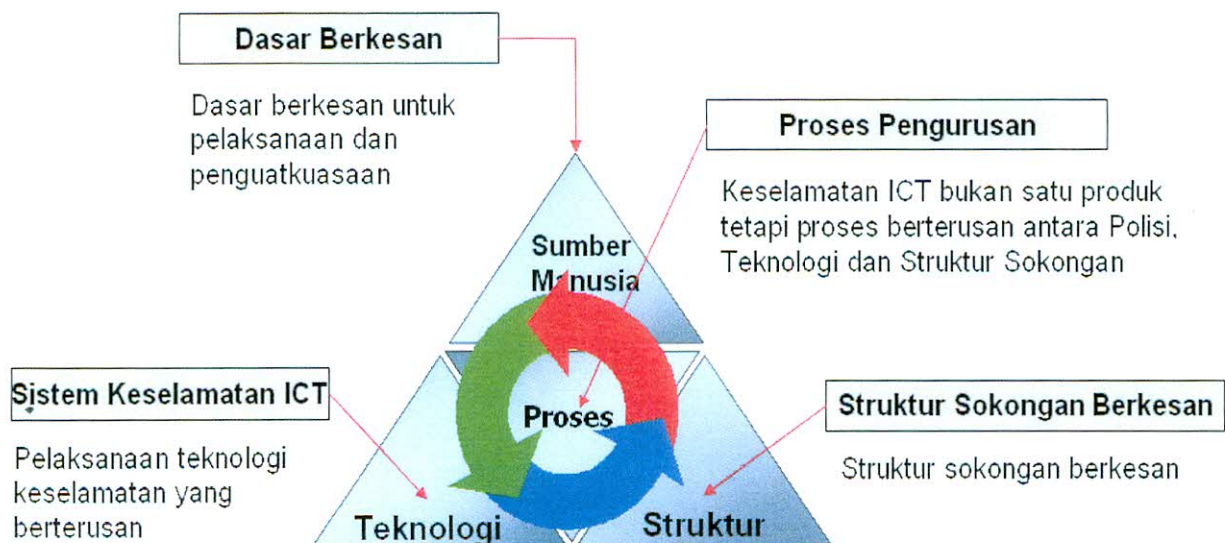


**MANUAL PENGURUSAN KESELAMATAN ICT TUDM**

**BAHAGIAN 1**

**MANUAL PENGURUSAN KESELAMATAN ICT TUDM****BAHAGIAN 1****RISALAH 1****PERNYATAAN DAN PERLAKSANAAN****PENDAHULUAN**

1. Penggunaan Teknologi Maklumat dan Komunikasi (ICT) secara komprehensif telah memberikan impak terhadap isu-isu keselamatan ICT. Aspek keselamatan ICT yang perlu diberikan perhatian merangkumi keselamatan informasi, keselamatan infrastruktur dan infostruktur berkaitan serta penguatkuasaannya. Ini memerlukan kesedaran dan komitmen yang tinggi di kalangan warga Tentera Udara DiRaja Malaysia (TUDM) terutamanya dari aspek peranan, tanggungjawab dan kawalan penggunaan sistem ICT, daripada sebarang penyalahgunaan dan ancaman pencerobohan.
2. Penguatkuasaan ke atas keselamatan ICT adalah kritikal dan perlu diberi penekanan yang serius sesuai dengan peranan TUDM sebagai organisasi yang bertanggungjawab dalam memastikan keselamatan negara terjamin. Pelaksanaan penguatkuasaan perlu berlandaskan Manual Keselamatan ICT (MKICT) TUDM yang berpandukan garis panduan daripada pihak MAMPU dan Dasar Keselamatan ICT MinDef seperti di **Rajah 1**.

**Rajah 1: Model Dasar Keselamatan ICT MinDef**



**TUJUAN**

3. MKICT TUDM diwujudkan sebagai garis panduan untuk memaksimumkan aspek keselamatan ICT merangkumi keselamatan informasi, keselamatan infrastruktur dan infostruktur bagi memenuhi keperluan operasi TUDM.

**OBJEKTIF**

4. Objektif Manual Keselamatan ICT TUDM ialah seperti berikut:
- a. Menyatakan pengarah dan hala tuju pihak pengurusan tertinggi untuk mendokong pelaksanaan keselamatan ICT.
  - b. Memastikan Keselamatan ICT TUDM terjamin, sesuai dengan perubahan semasa dan boleh digunapakai oleh semua peringkat pengurusan dan pengguna.
  - c. Melindungi kepentingan aset-aset dan pihak-pihak yang terlibat dengan sistem ICT TUDM daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi, pencerobohan serta mencegah aktiviti penyalahgunaan dan kecurian.
  - d. Memastikan kelancaran operasi TUDM dan meminimumkan kerosakan atau kemusnahan infostruktur TUDM.

**SASARAN**

5. Manual ini disasarkan kepada setiap warga TUDM dan awam KEMENTAH, pembekal, pakar runding dan pihak-pihak lain yang terlibat di dalam mengendalikan maklumat.

**MANUAL PENGURUSAN KESELAMATAN ICT TUDM****BAHAGIAN 1****RISALAH 2****PERNYATAAN MANUAL KESELAMATAN ICT TUDM****PENDAHULUAN**

1. Keselamatan ICT ditakrifkan sebagai keadaan yang bebas daripada sebarang ancaman, risiko pencemaran dan pencerobohan. Perlindungan daripada ancaman dan risiko memerlukan usaha yang berterusan bagi menjamin keselamatan ICT TUDM. Program yang perlu dilaksanakan melibatkan aktiviti pencegahan berkala bagi menghadapi sebarang bentuk ancaman.

**TUJUAN**

2. Pernyataan Manual Keselamatan ICT TUDM adalah bertujuan untuk memastikan segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan.

**KOMPONEN**

3. Keselamatan ICT adalah berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

- a. Melindungi maklumat kerahsiaan TUDM.
- b. Menjamin setiap maklumat adalah tepat.
- c. Memastikan ketersediaan maklumat.
- d. Memastikan akses hanya diwujudkan kepada pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

4. Manual Keselamatan ICT TUDM merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan



kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

- a. **Kerahsiaan.** Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.
  - b. **Integriti.** Data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan.
  - c. **Tidak Boleh Disangkal.** Punca data dan maklumat adalah dari punca yang sah dan tidak boleh disangkal.
  - d. **Kesahihan.** Data dan maklumat hendaklah dijamin kesahihannya.
  - e. **Ketersediaan.** Data dan maklumat hendaklah boleh diakses pada bila-bila masa.
5. MKICT TUDM merangkumi perlindungan ke atas semua bentuk maklumat kerajaan yang diwujudkan, dimasukkan, diedar, dijana, disimpan, dicetak, diakses dan dimusnah melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua aset ICT di lokasi yang terlibat. **Sebarang kebocoran rahsia atau keselamatan perlindungan adalah dianggap sebagai pelanggaran langkah-langkah keselamatan.**
6. Langkah-langkah ke arah menjamin keselamatan ICT adalah berpandukan kepada penilaian yang bersesuaian terhadap aspek berikut:
- a. Perubahan semasa terhadap kelemahan Sistem ICT.
  - b. Ancaman yang wujud akibat daripada kelemahan sistem.
  - c. Risiko yang mungkin timbul.
  - d. Teknik pencegahan yang boleh diambil untuk menangani risiko.

#### **PRINSIP-PRINSIP MANUAL KESELAMATAN ICT TUDM**

7. Prinsip-prinsip yang menjadi asas kepada Manual Keselamatan ICT TUDM adalah seperti berikut:
- a. Akses atas dasar "perlu mengetahui".
  - b. Hak akses minima.
  - c. Akauntabiliti.
  - d. Pengasingan Fungsi.

- e. Pengauditan Keselamatan.
- f. Pematuhan.
- g. Pemulihan.
- h. Saling bergantung.

### **AKSES ATAS MANUAL PERLU MENGETAHUI**

8. Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan akses di bawah prinsip ini adalah berasaskan kepada klasifikasi maklumat dan tapisan keselamatan pengguna seperti berikut:

- a. **Klasifikasi Maklumat.** Keselamatan ICT TUDM dikategorikan kepada Rahsia Besar, Rahsia, Sulit dan Terhad. Data, bahan atau maklumat rasmi yang sensitif atau bersifat terperingkat perlu dilindungi dari pendedahan, dimanipulasi atau diubah semasa dalam penghantaran. Penggunaan kod dan tandatangan digital mesti dipertimbangkan bagi melindungi data yang dikirim secara elektronik. Dasar kawalan akses ke atas aplikasi atau sistem juga hendaklah mengikut klasifikasi maklumat yang sama, iaitu sama ada Rahsia Besar, Rahsia, Sulit atau Terhad.
- b. **Tapisan Keselamatan Pengguna.** Hanya pengguna yang telah lulus tapisan keselamatan akan dibenarkan untuk mengakses maklumat mengikut klasifikasi keselamatan dan kategori maklumat yang ditetapkan.

### **HAK AKSES MINIMA**

9. Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujudkan, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu disemak dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.



**AKAUNTABILITI**

10. Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT TUDM. Untuk menentukan ianya dipatuhi, sistem ICT hendaklah mempunyai keupayaan untuk mengesan sebarang tindakan yang tidak mengikut Manual Keselamatan ICT.

11. Akauntabiliti atau tanggungjawab pengguna termasuklah:

- a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan.
- b. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa.
- c. Menentukan maklumat sedia untuk digunakan.
- d. Menjaga kerahsiaan kata laluan.
- e. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan.
- f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penyelenggaraan, penghantaran, penyampaian, pertukaran dan pemusnahan.

**PENGASINGAN FUNGSI**

12. Pengasingan fungsi perlu diadakan di antara pentadbir dan pengguna. Pengasingan fungsi juga hendaklah dilakukan di antara pentadbir sistem dan pentadbir rangkaian. Tugas mewujudkan, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi.

13. Pada tahap minima, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut:

- a. Persekitaran pembangunan di mana sesuatu aplikasi dalam proses pembangunan.
- b. Persekitaran penerimaan di mana sesuatu aplikasi diuji.
- c. Persekitaran sebenar di mana aplikasi sedia untuk beroperasi.

### **PENGAUDITAN KESELAMATAN**

14. Pengauditan keselamatan adalah:

- a. Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*. Pentingnya *audit trail* ini menjadi semakin ketara apabila wujud keperluan untuk mengenal pasti punca masalah atau ancaman kepada keselamatan ICT. Oleh itu, rekod audit hendaklah dilindungi dan tersedia untuk penilaian atau tindakan serta-merta.
- b. Pengauditan juga perlu dibuat ke atas rekod-rekod manual seperti dokumen operasi, nota serah tugas, kelulusan keluar pejabat, memorandum, borang kebenaran, surat kuasa, senarai inventori dan kemudahan akses log. Ini adalah kerana dalam kes-kes tertentu, dokumen ini diperlukan untuk menyokong *audit trail* sistem komputer.
- c. Keseluruhannya, sistem pengauditan ini adalah penting dalam menjamin akauntabiliti. Antara lain, sistem ini dapat dirujuk bagi menentukan perkara-perkara berikut:
  - (1) Mengesan pematuhan atau pelanggaran keselamatan.
  - (2) Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya pelanggaran keselamatan.



- (3) Menyediakan bahan bukti bagi menentukan sama ada berlakunya pelanggaran keselamatan.

### **PEMATUHAN**

15. MKICT TUDM hendaklah difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.
16. Pematuhan MKICT TUDM adalah berdasarkan tindakan berikut:
- a. Mewujudkan proses yang sistematik khususnya untuk menjamin keselamatan ICT bagi memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan.
  - b. Merumus pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenalpasti.
  - c. Pelaksanaan program pengawasan dan pemantauan keselamatan maklumat secara berterusan hendaklah dilaksanakan oleh setiap perkhidmatan di kawasan tanggungjawab masing-masing.
  - d. Menguatkuasakan amalan melapor sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan.

### **PEMULIHAN**

17. Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian maklumat. Objektif utama adalah untuk meminimalkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Antara lain, pemulihan boleh dilakukan melalui tindakan-tindakan berikut:
- a. Merumus dan menguji Pelan Pemulihan Bencana/Kesinambungan perkhidmatan – (*Disaster Recovery Plan*).
  - b. Mengamalkan langkah-langkah membuat salinan data dan lain-lain amalan terbaik dalam penggunaan ICT seperti menghapuskan virus, langkah-langkah pencegahan kebakaran dan amalan *clear desk and clear screen*.

**SALING BERGANTUNG**

18. Langkah-langkah keselamatan ICT yang berkesan memerlukan pematuhan kepada semua prinsip-prinsip di atas. Setiap prinsip adalah saling lengkap-melengkapi antara satu dengan lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorak sebanyak mungkin mekanisma keselamatan, dapat menjamin keselamatan yang maksima. Prinsip saling bergantung meliputi beberapa peringkat di mana mengandungi langkah-langkah berikut:

- a. **Sambungan Kepada Internet.** Semua komputer yang hendak dihubungkan dengan internet mestilah mendapatkan kelulusan BTMK. Ancaman dan bahaya keselamatan maklumat mestilah dipantau dan diuruskan dengan berkesan. Semua trafik dari luar ke dalam mestilah dikawal dengan menyediakan *firewall*.
- b. **Backbone Rangkaian.** *Backbone* rangkaian akan hanya mengendalikan trafik yang telah dikod untuk melindungi setiap maklumat yang dihantar.
- c. **Rangkaian Jabatan.** Semua rangkaian jabatan akan dihubungkan ke *backbone* melalui *firewall* yang mana akan pula mengkod semua trafik di antara rangkaian jabatan dengan rangkaian di peringkat yang seterusnya atau pusat data.
- d. **Pelayan Jabatan.** Semua data dan maklumat yang berdarjah akan hanya disimpan di pelayan jabatan atau di pelayan yang diurus secara pusat bagi menghindar pendedahan, pengubahan atau kecurian.

**SKOP MANUAL KESELAMATAN ICT TUDM**

19. Bagi menentukan Sistem ICT ini terjamin keselamatannya sepanjang masa, Manual Keselamatan ICT TUDM ini diwujudkan merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujudkan, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan keselamatan ke dalam semua aset ICT. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:



a. **Perkakasan.** Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan TUDM seperti komputer, pelayan, peralatan komunikasi dan sebagainya.

b. **Perisian.** Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada TUDM.

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

(1) Rangkaian seperti LAN, WAN dan lain-lain.

(2) Sistem halangan akses seperti sistem kad akses.

(3) Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

d. **Data dan Maklumat.** Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif perkhidmatan. Contoh: Sistem dokumentasi, prosedur operasi, rekod-rekod TUDM, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain.

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

(2) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketetapan maklumat serta untuk melindungi kepentingan TUDM, perkhidmatan dan masyarakat.

e. **Manusia.** Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian bagi mencapai misi dan objektif TUDM. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

f. **Premis Komputer Dan Komunikasi.** Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a) - (e) di atas.

g. Proses dan prosedur keselamatan ICT.

h. Tadbir urus keselamatan ICT.

20. Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai pelanggaran langkah-langkah keselamatan.

21. Di samping itu, Manual Keselamatan ICT TUDM ini juga adalah saling lengkap-melengkapi dan perlu dilaksanakan secara konsisten dengan undang-undang dan peraturan yang sedia ada.



**MANUAL PENGURUSAN KESELAMATAN ICT TUDM****BAHAGIAN 1****RISALAH 2****PERNYATAAN MANUAL KESELAMATAN ICT TUDM****PENDAHULUAN**

1. Keselamatan ICT ditakrifkan sebagai keadaan yang bebas daripada sebarang ancaman, risiko pencemaran dan pencerobohan. Perlindungan daripada ancaman dan risiko memerlukan usaha yang berterusan bagi menjamin keselamatan ICT TUDM. Program yang perlu dilaksanakan melibatkan aktiviti pencegahan berkala bagi menghadapi sebarang bentuk ancaman.

**TUJUAN**

2. Pernyataan Manual Keselamatan ICT TUDM adalah bertujuan untuk memastikan segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan.

**KOMPONEN**

3. Keselamatan ICT adalah berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

- a. Melindungi maklumat kerahsiaan TUDM.
- b. Menjamin setiap maklumat adalah tepat.
- c. Memastikan ketersediaan maklumat.
- d. Memastikan akses hanya diwujudkan kepada pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

4. Manual Keselamatan ICT TUDM merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

- a. **Kerahsiaan.** Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.
  - b. **Integriti.** Data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan.
  - c. **Tidak Boleh Disangkal.** Punca data dan maklumat adalah dari punca yang sah dan tidak boleh disangkal.
  - d. **Kesahihan.** Data dan maklumat hendaklah dijamin kesahihannya.
  - e. **Ketersediaan.** Data dan maklumat hendaklah boleh diakses pada bila-bila masa.
5. MKICT TUDM merangkumi perlindungan ke atas semua bentuk maklumat kerajaan yang diwujudkan, dimasukkan, diedar, dijana, disimpan, dicetak, diakses dan dimusnah melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua aset ICT di lokasi yang terlibat. **Sebarang kebocoran rahsia atau keselamatan perlindungan adalah dianggap sebagai pelanggaran langkah-langkah keselamatan.**
6. Langkah-langkah ke arah menjamin keselamatan ICT adalah berpandukan kepada penilaian yang bersesuaian terhadap aspek berikut:
- a. Perubahan semasa terhadap kelemahan Sistem ICT.
  - b. Ancaman yang wujud akibat daripada kelemahan sistem.
  - c. Risiko yang mungkin timbul.
  - d. Teknik pencegahan yang boleh diambil untuk menangani risiko.

#### **PRINSIP-PRINSIP MANUAL KESELAMATAN ICT TUDM**

7. Prinsip-prinsip yang menjadi asas kepada Manual Keselamatan ICT TUDM adalah seperti berikut:
- a. Akses atas dasar "perlu mengetahui".
  - b. Hak akses minima.
  - c. Akauntabiliti.
  - d. Pengasingan Fungsi.
  - e. Pengauditan Keselamatan.
  - f. Pematuhan.
  - g. Pemulihan.
  - h. Saling bergantung.



**AKSES ATAS MANUAL PERLU MENGETAHUI**

8. Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan akses di bawah prinsip ini adalah berasaskan kepada klasifikasi maklumat dan tapisan keselamatan pengguna seperti berikut:

a. **Klasifikasi Maklumat.** Keselamatan ICT TUDM dikategorikan kepada Rahsia Besar, Rahsia, Sulit dan Terhad. Data, bahan atau maklumat rasmi yang sensitif atau bersifat terperingkat perlu dilindungi dari pendedahan, dimanipulasi atau diubah semasa dalam penghantaran. Penggunaan kod dan tandatangan digital mesti dipertimbangkan bagi melindungi data yang dikirim secara elektronik. Dasar kawalan akses ke atas aplikasi atau sistem juga hendaklah mengikut klasifikasi maklumat yang sama, iaitu sama ada Rahsia Besar, Rahsia, Sulit atau Terhad.

b. **Tapisan Keselamatan Pengguna.** Hanya pengguna yang telah lulus tapisan keselamatan akan dibenarkan untuk mengakses maklumat mengikut klasifikasi keselamatan dan kategori maklumat yang ditetapkan.

**HAK AKSES MINIMA**

9. Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujudkan, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu disemak dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

**AKAUNTABILITI**

10. Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT TUDM. Untuk menentukan ianya dipatuhi, sistem ICT hendaklah mempunyai keupayaan untuk mengesan sebarang tindakan yang tidak mengikut Manual Keselamatan ICT.

11. Akauntabiliti atau tanggungjawab pengguna termasuklah:
- Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan.
  - Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa.
  - Menentukan maklumat sedia untuk digunakan.
  - Menjaga kerahsiaan kata laluan.
  - Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan.
  - Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penyelenggaraan, penghantaran, penyampaian, pertukaran dan pemusnahan.

#### **PENGASINGAN FUNGSI**

12. Pengasingan fungsi perlu diadakan di antara pentadbir dan pengguna. Pengasingan fungsi juga hendaklah dilakukan di antara pentadbir sistem dan pentadbir rangkaian. Tugas mewujudkan, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi.

13. Pada tahap minima, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut:

- Persekitaran pembangunan di mana sesuatu aplikasi dalam proses pembangunan.
- Persekitaran penerimaan di mana sesuatu aplikasi diuji.
- Persekitaran sebenar di mana aplikasi sedia untuk beroperasi.



**PENGAUDITAN KESELAMATAN**

14. Pengauditan keselamatan adalah:

a. Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*. Pentingnya *audit trail* ini menjadi semakin ketara apabila wujud keperluan untuk mengenal pasti punca masalah atau ancaman kepada keselamatan ICT. Oleh itu, rekod audit hendaklah dilindungi dan tersedia untuk penilaian atau tindakan serta-merta.

b. Pengauditan juga perlu dibuat ke atas rekod-rekod manual seperti dokumen operasi, nota serah tugas, kelulusan keluar pejabat, memorandum, borang kebenaran, surat kuasa, senarai inventori dan kemudahan akses log. Ini adalah kerana dalam kes-kes tertentu, dokumen ini diperlukan untuk menyokong *audit trail* sistem komputer.

c. Keseluruhannya, sistem pengauditan ini adalah penting dalam menjamin akauntabiliti. Antara lain, sistem ini dapat dirujuk bagi menentukan perkara-perkara berikut:

- (1) Mengesan pematuhan atau pelanggaran keselamatan.
- (2) Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya pelanggaran keselamatan.
- (3) Menyediakan bahan bukti bagi menentukan sama ada berlakunya pelanggaran keselamatan.

**PEMATUHAN**

15. MKICT TUDM hendaklah difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

16. Pematuhan MKICT TUDM adalah berdasarkan tindakan berikut:
- a. Mewujudkan proses yang sistematik khususnya untuk menjamin keselamatan ICT bagi memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan.
  - b. Merumus pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenalpasti.
  - c. Pelaksanaan program pengawasan dan pemantauan keselamatan maklumat secara berterusan hendaklah dilaksanakan oleh setiap perkhidmatan di kawasan tanggungjawab masing-masing.
  - d. Menguatkuasakan amalan melapor sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan.

### **PEMULIHAN**

17. Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian maklumat. Objektif utama adalah untuk meminimalkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Antara lain, pemulihan boleh dilakukan melalui tindakan-tindakan berikut:

- a. Merumus dan menguji Pelan Pemulihan Bencana/Kesinambungan perkhidmatan – (*Disaster Recovery Plan*).
- b. Mengamalkan langkah-langkah membuat salinan data dan lain-lain amalan terbaik dalam penggunaan ICT seperti menghapuskan virus, langkah-langkah pencegahan kebakaran dan amalan *clear desk and clear screen*.

### **SALING BERGANTUNG**

18. Langkah-langkah keselamatan ICT yang berkesan memerlukan pematuhan kepada semua prinsip-prinsip di atas. Setiap prinsip adalah saling lengkap-melengkapi antara satu dengan lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorak sebanyak mungkin mekanisma keselamatan, dapat menjamin keselamatan yang maksima. Prinsip saling bergantung meliputi beberapa peringkat di mana mengandungi langkah-langkah berikut:



- a. **Sambungan Kepada Internet.** Semua komputer yang hendak dihubungkan dengan internet mestilah mendapatkan kelulusan BTMK. Ancaman dan bahaya keselamatan maklumat mestilah dipantau dan diuruskan dengan berkesan. Semua trafik dari luar ke dalam mestilah dikawal dengan menyediakan *firewall*.
- b. **Backbone Rangkaian.** *Backbone* rangkaian akan hanya mengendalikan trafik yang telah dikod untuk melindungi setiap maklumat yang dihantar.
- c. **Rangkaian Jabatan.** Semua rangkaian jabatan akan dihubungkan ke *backbone* melalui *firewall* yang mana akan pula mengkod semua trafik di antara rangkaian jabatan dengan rangkaian di peringkat yang seterusnya atau pusat data.
- d. **Pelayan Jabatan.** Semua data dan maklumat yang berdarjah akan hanya disimpan di pelayan jabatan atau di pelayan yang diurus secara pusat bagi menghindar pendedahan, pengubahan atau kecurian.

#### **SKOP MANUAL KESELAMATAN ICT TUDM**

19. Bagi menentukan Sistem ICT ini terjamin keselamatannya sepanjang masa, Manual Keselamatan ICT TUDM ini diwujudkan merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujudkan, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan keselamatan ke dalam semua aset ICT. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

- a. **Perkakasan.** Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan TUDM seperti komputer, pelayan, peralatan komunikasi dan sebagainya.
- b. **Perisian.** Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada TUDM.
- c. **Perkhidmatan.** Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:

- (1) Rangkaian seperti LAN, WAN dan lain-lain.
- (2) Sistem halangan akses seperti sistem kad akses.
- (3) Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

d. **Data dan Maklumat.** Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif perkhidmatan. Contoh: Sistem dokumentasi, prosedur operasi, rekod-rekod TUDM, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain.

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

(2) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketetapan maklumat serta untuk melindungi kepentingan TUDM, perkhidmatan dan masyarakat.

e. **Manusia.** Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian bagi mencapai misi dan objektif TUDM. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

f. **Premis Komputer Dan Komunikasi.** Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a) - (e) di atas.

g. Proses dan prosedur keselamatan ICT.

h. Tadbir urus keselamatan ICT.



20. Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai pelanggaran langkah-langkah keselamatan.

21. Di samping itu, Manual Keselamatan ICT TUDM ini juga adalah saling lengkap-melengkapi dan perlu dilaksanakan secara konsisten dengan undang-undang dan peraturan yang sedia ada.

**MANUAL PENGURUSAN KESELAMATAN ICT TUDM****BAHAGIAN 1****RISALAH 3****PELAKSANAAN MANUAL KESELAMATAN ICT TUDM****PENDAHULUAN**

1. Setiap entiti dalam TUDM hendaklah melaksanakan manual tersebut bagi menjamin perlindungan ke atas kerahsiaan, integriti dan kebolehsediaan maklumat dan seterusnya menjamin kesinambungan urusan dan perkhidmatan dengan meminimumkan kesan insiden keselamatan.

**TUJUAN**

2. Memberi hala tuju dan peraturan-peraturan bagi mengguna dan melindungi aset ICT selaras dengan keperluan undang-undang.

**PELAKSANAAN MANUAL KESELAMATAN ICT TUDM**

3. Pelaksanaan manual ini akan dijalankan oleh Jawatankuasa keselamatan ICT TUDM yang terdiri daripada Ketua Pegawai Maklumat (CIO – Timbalan Panglima Tentera Udara(TPTU)), Pegawai Keselamatan ICT (ICTSO – Pengarah BTMK) dan lain-lain pegawai yang dilantik.

**PENYEBARAN MANUAL**

4. Manual ini perlu disebar kepada semua pengguna TUDM (termasuk staf, pembekal dan pakar runding yang berurusan dengan TUDM).

**SEMAKAN MANUAL**

5. Manual Keselamatan ICT TUDM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur perundangan, dasar kerajaan dan kepentingan sosial.

6. Prosedur semakan Manual Keselamatan ICT TUDM adalah termasuk yang berikut:



- a. Menyemak manual ini sekurang-kurangnya sekali setahun bagi mengenalpasti dan menentukan perubahan yang diperlukan.
- b. Mengemukakan cadangan perubahan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Jawatankuasa Keselamatan ICT TUDM.
- c. Memaklumkan perubahan manual yang telah dipersetujui oleh Jawatankuasa Keselamatan ICT TUDM kepada semua pengguna.

#### **PEMATUHAN MANUAL KESELAMATAN ICT TUDM**

- 7. Manual Keselamatan ICT TUDM perlu dipatuhi oleh semua pengguna aset ICT termasuk pihak ketiga yang berurusan dengan kerajaan dan tiada pengecualian diberikan.

**MANUAL PENGURUSAN KESELAMATAN ICT TUDM**

**BAHAGIAN 2**



**MANUAL PENGURUSAN KESELAMATAN ICT TUDM****BAHAGIAN 2****RISALAH 1****PENGURUSAN KESELAMATAN ICT TUDM****PENDAHULUAN**

1. Rangka kerja pengurusan keselamatan ICT diwujudkan supaya keselamatan ICT dilaksanakan dengan lebih sistematik, lancar dan berkesan.

**TUJUAN**

2. Menerangkan peranan dan tanggungjawab organisasi pengurusan keselamatan ICT dan individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Manual Keselamatan ICT TUDM.

**KETUA PEGAWAI MAKLUMAT**

3. Ketua Pegawai Maklumat (CIO) TUDM ialah Timbalan Panglima Tentera Udara (TPTU). Peranan dan tanggungjawab CIO adalah seperti berikut:
  - a. Memastikan organisasi keselamatan ICT TUDM berfungsi dengan berkesan.
  - b. Memastikan semua pengguna memahami dan mematuhi Manual Keselamatan ICT TUDM.
  - c. Memastikan semua keperluan keselamatan ICT (sumber kewangan, staf dan perlindungan keselamatan) adalah mencukupi.
  - d. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Manual Keselamatan ICT TUDM.
  - e. Menyelaraskan pembangunan dan pelaksanaan pelan tindakan dan program kesedaran mengenai keselamatan ICT.
  - f. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT.

- g. Mempengerusikan Mesyuarat Jawatankuasa ICT TUDM.

#### **PEGAWAI KESELAMATAN ICT**

4. Pegawai Keselamatan ICT (ICTSO) bagi TUDM adalah Pengarah Bahagian Teknologi Maklumat & Komunikasi (BTMK). Peranan dan tanggungjawab ICTSO adalah seperti berikut:

- a. Menguatkuasa dan memantau pematuhan Manual Keselamatan ICT TUDM.
- b. Mengurus keseluruhan program-program keselamatan ICT TUDM.
- c. Memberi penerangan dan pendedahan berkenaan Manual Keselamatan ICT TUDM kepada semua pengguna.
- d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Manual Keselamatan ICT TUDM.
- e. Menjalankan tugas pengurusan risiko.
- f. Menjalankan audit, mengkaji, merumus tindakbalas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya.
- g. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti *malware* dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian.
- h. Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan (G\*CERT), MAMPU dan memaklukkannya kepada CIO.
- i. Bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baikpulih dengan segera.
- j. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.

**PENGURUS ICT**

5. Pengurus ICT bagi TUDM ialah pegawai ICT yang dilantik di BTMK. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:

- a. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan TUDM.
- b. Menentukan kawalan akses semua pengguna terhadap aset ICT TUDM.
- c. Melaporkan sebarang insiden atau penemuan ancaman keselamatan ICT kepada TUDM\*CERT.
- d. Memastikan penyimpanan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT TUDM.

**PENTADBIR SISTEM ICT**

6. Pentadbir Sistem ICT bagi TUDM ialah pegawai ICT yang dilantik oleh BTMK. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut :

- a. Memastikan kerahsiaan kata laluan aset ICT.
- b. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pengguna ICT TUDM yang berhenti, bersara, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas.
- c. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pengguna luar dan pihak ketiga yang berhenti atau tamat projek.
- d. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Manual Keselamatan ICT TUDM.
- e. Memantau aktiviti capaian harian sistem aplikasi pengguna.
- f. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dengan membatalkan atau memberhentikan



dengan serta merta capaian terhadap sistem dan memaklumkan kepada Pengurus ICT untuk tindakan selanjutnya.

- g. Menganalisa dan menyimpan rekod jejak audit.
- h. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.
- i. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.

### **PENGGUNA**

7. Pengguna ditakrifkan sebagai individu yang mengakses aset ICT TUDM termasuklah kakitangan dan bukan kakitangan yang bertugas atau berurusan dengan sistem ICT TUDM. Peranan dan tanggungjawab pengguna adalah seperti berikut:

- a. Membaca, memahami dan mematuhi Manual Keselamatan ICT TUDM.
- b. Mengetahui dan memahami implikasi keselamatan ICT akibat dari tindakannya.
- c. Menjalani proses tapisan keselamatan seperti yang diarahkan.
- d. Mematuhi prinsip-prinsip Manual Keselamatan ICT TUDM dan menjaga kerahsiaan maklumat TUDM.
- e. Melaksanakan langkah-langkah perlindungan seperti 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 kata laluan.
  - (5) Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan.
  - (6) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan.
  - (7) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.
- f. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada TUDM\*CERT dengan segera.
- g. Menghadiri program-program kesedaran mengenai keselamatan ICT.

#### **KONTRAKTOR / PIHAK KETIGA**

8. Pihak TUDM hendaklah memastikan keselamatan pengguna maklumat dan kemudahan proses maklumat oleh kontraktor/pihak ketiga dikawal. Perkara yang perlu dipatuhi adalah seperti berikut:

- a. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian.
- b. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pengguna luar/asing. Capaian kepada aset ICT TUDM perlu berlandaskan kepada perjanjian kontrak.
- c. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga.
- d. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai:

- (1) Manual Keselamatan ICT TUDM.

- (2) Tapisan Keselamatan.
- (3) Akta Rahsia Rasmi 1986 (Pindaan).
- (4) Hak Harta Intelek.

**JAWATANKUASA ICT TUDM (JKICT TUDM)**

9. JKICT TUDM adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT TUDM.

10. Keanggotaan JKICT TUDM adalah seperti berikut:

**Pengerusi** : Timbalan Panglima Tentera Udara (CIO)

**Ahli** :

- a. Semua AKS
- b. Pengarah BTMK
- c. Semua PS 1 BTMK
- d. Lain-lain yang diperlukan.

11. Urus Setia bagi JKICT TUDM ialah Bahagian Teknologi Maklumat dan Komunikasi - BTMK.

**Bidang Kuasa** :

- a. Memperaku, melulus dan menguatkuasakan dasar, halatuju, garis panduan dan piawaian keselamatan ICT.
- b. Memantau tahap pematuhan keselamatan ICT.
- c. Memastikan Manual Keselamatan ICT TUDM selaras dengan dasar-dasar ICT semasa kerajaan.



- d. Menerima dan membincangkan laporan mengenai insiden-insiden keselamatan ICT semasa.
- e. Membincang tindakan yang melibatkan pelanggaran Manual Keselamatan ICT TUDM.
- f. Meneliti dan meluluskan semua program dan aktiviti yang berkaitan dengan keselamatan ICT.
- g. Memastikan pengauditan keselamatan ICT TUDM dilaksanakan sekurang-kurangnya sekali setahun.
- h. Memastikan peruntukkan kewangan yang mencukupi disediakan untuk pelaksanaan program dan aktiviti keselamatan.

12. BTMK yang berperanan sebagai sekretariat Jawatankuasa Pengurusan Keselamatan ICT TUDM adalah bertanggungjawab bagi:

- a. Mewujudkan Pelan Strategik ICT TUDM.
- b. Membangun dan menyelaraskan pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT TUDM.
- c. Memastikan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Manual Keselamatan ICT TUDM.
- d. Menyelaraskan pelaksanaan pengurusan risiko dan audit keselamatan.
- e. Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlaku ancaman yang berbahaya seperti virus dan menyediakan khidmat nasihat serta langkah pemulihan yang bersesuaian.

**ORGANISASI ROYAL MALAYSIAN AIR FORCE (RMAF) COMPUTER  
EMERGENCY RESPONSE TEAM (TUDM\*CERT)**

13. Keanggotaan TUDM\*CERT adalah seperti berikut:

**Pengerusi TUDM\*CERT :** Pengarah TMK (ICTSO)

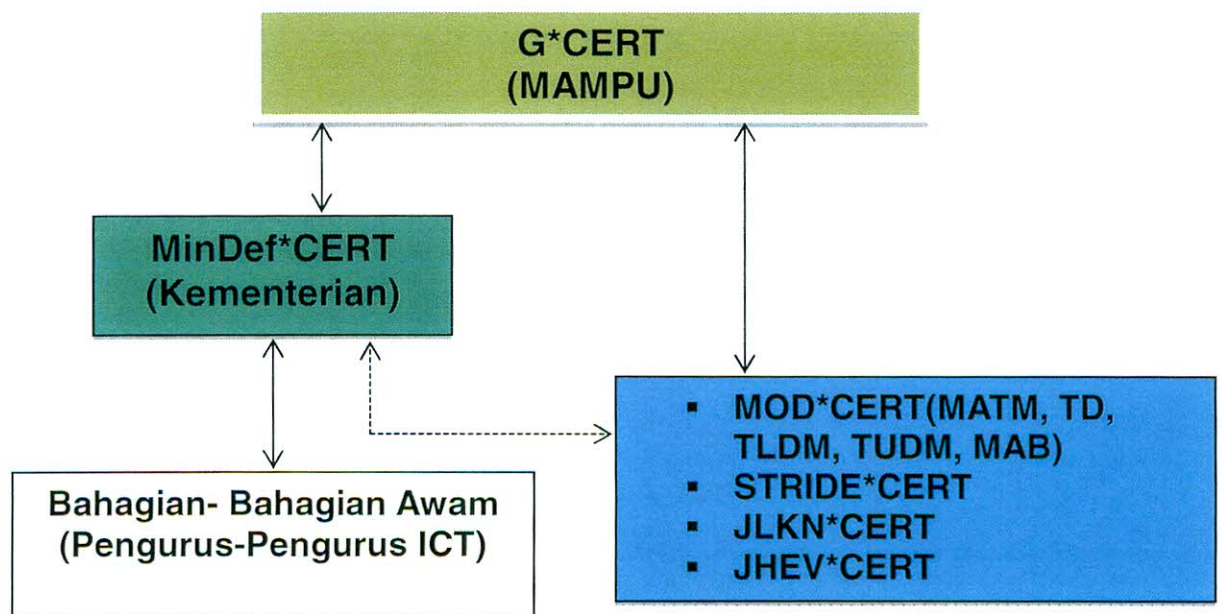
**Ahli :**

- a. PS 1 TM (Setiausaha).
- b. PS 1 Operasi.
- c. PS 1 Aplikasi.
- d. PS 1 P4.
- e. PS 1 Peperangan Maklumat.
- f. PS 1 Komunikasi.
- g. Lain-lain yang diperlukan.

**Bidang Kuasa :** Tanggungjawab TUDM\*CERT meliputi semua bidang tugas pengurusan pengendalian insiden keselamatan ICT yang dialami oleh TUDM. Tugas-tugas TUDM\*CERT adalah seperti berikut:

- a. Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden.
- b. Merekod dan menjalankan siasatan awal insiden yang diterima.
- c. Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baikpulih minima.

- d. Menghubungi dan melapor insiden yang berlaku kepada MinDef\***CERT** dan G\***CERT** MAMPU sama ada input atau untuk tindakan seterusnya.
- e. Menasihati Markas dan Pangkalan TUDM mengambil tindakan pemulihan dan pengukuhan.
- f. Memaklumkan sebarang ancaman dan insiden keselamatan ICT kepada Markas dan Pangkalan TUDM.
- g. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.



**Rajah 2: Carta Pelaporan Insiden Keselamatan ICT TUDM**

14. Semua insiden keselamatan ICT yang berlaku di Markas dan Pangkalan TUDM perlu dilaporkan kepada TUDM\***CERT**. TUDM\***CERT** akan melaporkan terus ke G\***CERT** MAMPU dan dimaklumkan kepada MinDef\***CERT**.



**MANUAL PENGURUSAN KESELAMATAN ICT TUDM****BAHAGIAN 2****RISALAH 2****PENGURUSAN ASET****PENDAHULUAN**

1. Aset ICT TUDM terdiri daripada peralatan komputer dan komunikasi. Pengurusan aset ICT TUDM perlu dilaksanakan secara sistematik dengan memberi penekanan kepada aspek-aspek senggaraan dan aspek-aspek kerahsiaan serta mengikut tatacara yang telah ditetapkan oleh kerajaan. Prosedur bagi pengurusan aset ICT TUDM dalam pengawalan dan perlindungan yang perlu dipatuhi.

**TUJUAN**

2. Untuk memastikan semua aset ICT TUDM diuruskan dengan cekap dan berada di tahap optima.

**TANGGUNGJAWAB KE ATAS ASET**

3. Memastikan semua aset ICT TUDM diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang inventori masing-masing. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut:

- a. Memastikan semua aset dikenalpasti dan maklumat aset direkod dalam Borang Daftar Harta Modal serta sentiasa dikemaskini.
- b. Memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja.
- c. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.
- d. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di TUDM.

- e. Peraturan bagi pengendalian aset hendaklah dikenalpasti, di dokumenkan dan dipatuhi.

### **PENGELASAN MAKLUMAT**

4. Memastikan setiap maklumat diberi perlindungan yang bersesuaian berdasarkan tahap kerahsiaan.
5. Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada kerajaan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut:

- a. Rahsia Besar.
- b. Rahsia.
- c. Sulit.
- d. Terhad.

### **PELABELAN DAN PENGENDALIAN MAKLUMAT**

6. Pelabelan dan pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan hendaklah mengikut piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan. Prosedur pengurusan maklumat adalah mengikut jenis-jenis pemprosesan berikut :

- a. Penyalinan (*copying*).
- b. Storan.
- c. Penghantaran melalui pos, faks dan *e-mail*.
- d. Penghantaran melalui percakapan termasuk melalui telefon bimbit, mel suara dan mesin menjawab telefon.

e. Penghapusan.

f. Multimedia.

|                 | RAHSIA<br>BESAR | RAHSIA | SULIT | TERHAD | TERBUKA |
|-----------------|-----------------|--------|-------|--------|---------|
| 1. PENYALINAN   | AK              | AK     | AK    | BIASA  | BIASA   |
| 2. STORAN       | AK              | AK     | AK    | BIASA  | BIASA   |
| 3.TX-PERSURATAN | AK              | AK     | AK    | BIASA  | BIASA   |
| 4.TX-PERCAKAPAN | AK              | AK     | AK    | BIASA  | BIASA   |
| 5. PEMUSNAHAN   | AK              | AK     | AK    | BIASA  | BIASA   |
| 6. MULTIMEDIA   | AK              | AK     | AK    | BIASA  | BIASA   |

**Rajah 3 : Skim Penandaan Maklumat**

Nota :-

- a. **AK** – Arahan Khas
- b. **BIASA** - Terbuka iaitu Boleh dilakukan
- c. **TX** – Transmisi

7. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:

- a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan.
- b. Memeriksa, menyemak dan menentukan ketepatan maklumat sentiasa dikemaskini dan lengkap dari semasa ke semasa.
- c. Memastikan maklumat sedia untuk digunakan.
- d. Menjaga kerahsiaan kata laluan.
- e. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang dikeluarkan dari semasa ke semasa.



- f. Memberi perhatian kepada pengendalian maklumat rasmi terperingkat terutama semasa pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan.
- g. Menjaga kerahsiaan langkah-langkah pengurusan pengendalian maklumat rasmi keselamatan ICT dari diketahui umum.

**MANUAL PENGURUSAN KESELAMATAN ICT TUDM****BAHAGIAN 2****RISALAH 3****KESELAMATAN PERSONEL****PENDAHULUAN**

1. Markas/Pangkalan/Unit perlu memastikan setiap personel yang mengendalikan aset ICT memahami dan mematuhi tatacara keselamatan ICT yang digariskan. Pemerintah bertanggungjawab dalam pengendalian aset ICT di bawah kawalannya dan mengambil tindakan sewajarnya bagi menentukan pematuhan Manual Keselamatan ICT (MKICT) TUDM.

**TUJUAN**

2. Mewujudkan kesedaran dan pemahaman mengenai peranan dan tanggungjawab personel untuk mematuhi MKICT bagi meminimumkan risiko kesilapan, kecuaiian, kecurian, penipuan dan penyalahgunaan aset ICT.

**TANGGUNGJAWAB KESELAMATAN**

3. Peranan dan tanggungjawab semua personel yang terlibat dalam ICT TUDM termasuk pembekal, pakar runding dan pihak-pihak lain hendaklah jelas dan didokumenkan mengikut keperluan MKICT. Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- a. Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.
- b. Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, direkod, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau terma kontrak.
- c. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.

**TERMA PERKHIDMATAN**4. Anggota Tentera dan Awam :

- a. Anggota tentera dan awam yang menggunakan dan mengendalikan aset ICT dan maklumat elektronik berdarjah mestilah menjalani dan lulus tapisan keselamatan.
- b. Anggota tentera dan awam mesti mematuhi prosedur penggunaan aset ICT yang disediakan oleh setiap bahagian atau semua peringkat pemerintahan.

5. Pekerja Kontrak :

- a. Pekerja kontrak (berkhidmat secara kontrak) yang menggunakan aset ICT berkaitan tugas masing-masing sepanjang tempoh kontrak mestilah menjalani dan lulus tapisan keselamatan.
- b. Pekerja kontrak hendaklah mematuhi prosedur penggunaan aset ICT yang disediakan oleh setiap bahagian atau semua peringkat pemerintahan.

6. Kontraktor atau Pihak Ketiga. Kontraktor hanya dibenarkan menggunakan peralatan, terminal-terminal dan melakukan penyenggaraan terhadap peralatan yang mengikut kontrak untuk disenggara atau dibaiki dan hendaklah diawasi oleh anggota yang bertanggungjawab terhadap sistem atau projek tersebut.**SEBELUM MEMBERI PERKHIDMATAN**

## 7. Anggota tentera, anggota awam, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan perlu memahami tanggungjawab masing-masing ke atas keselamatan ICT. Perkara-perkara yang mesti dilaksanakan oleh Markas/Pangkalan/Unit adalah seperti berikut:

- a. Memberi penerangan dengan lengkap dan jelas mengenai peranan dan tanggungjawab pegawai dan anggota TUDM serta pihak ketiga yang terlibat bagi menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan.



- b. Menguruskan tapisan keselamatan untuk anggota TUDM serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan arahan semasa selaras dengan keperluan perkhidmatan.
- c. Memastikan pematuhan semua terma dan syarat perkhidmatan berdasarkan peraturan semasa.

#### **DALAM PERKHIDMATAN**

8. Anggota TUDM, anggota awam, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan perlu peka terhadap ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk mematuhi MKICT. Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- a. Memastikan pengurusan keselamatan aset ICT berdasarkan perundangan dan peraturan semasa yang ditetapkan oleh TUDM.
- b. Memastikan latihan kesedaran berkaitan dengan pengurusan keselamatan aset ICT diberi kepada pengguna ICT TUDM dan pihak ketiga secara berterusan.
- c. Memastikan tindakan disiplin dan/atau undang-undang ke atas anggota TUDM serta pihak ketiga yang berkepentingan sekiranya berlaku pelanggaran perundangan dan peraturan yang ditetapkan oleh TUDM.
- d. Memantapkan pengetahuan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul.

#### **BERTUKAR ATAU TAMAT PERKHIDMATAN**

9. Sebarang pertukaran atau tamat perkhidmatan yang melibatkan anggota TUDM, anggota awam, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan hendaklah diurus dengan teratur. Perkara-perkara yang perlu dipatuhi termasuk yang berikut :

- a. Memastikan semua aset ICT dikembalikan kepada TUDM mengikut peraturan yang ditetapkan oleh TUDM dan/atau klausa kontrak.

- b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh TUDM dan/atau klausa kontrak.

**MANUAL PENGURUSAN KESELAMATAN ICT TUDM****BAHAGIAN 2****RISALAH 4****KESELAMATAN FIZIKAL DAN PERSEKITARAN****PENDAHULUAN**

1. Premis dan peralatan ICT yang kritikal dan sensitif hendaklah ditempatkan di kawasan yang selamat dan dilindungi dari sebarang ancaman fizikal dan persekitaran.

**TUJUAN**

2. Menjamin keselamatan fizikal dan persekitaran aset ICT TUDM dari sebarang ancaman.

**KESELAMATAN FIZIKAL DAN PERSEKITARAN**

3. Markas/Pangkalan/Unit adalah bertanggungjawab untuk mengesan, mencegah dan menghalang pencerobohan ke atas kawasan yang menempatkan peralatan ICT dan maklumat.

**KAWALAN KAWASAN FIZIKAL**

4. Bertujuan untuk mengesan, mencegah dan menghalang cubaan menceroboh ke kawasan yang menempatkan peralatan ICT dan maklumat. Perkara yang perlu dipatuhi adalah seperti berikut:

- a. Mengenalpasti lokasi keselamatan fizikal dengan jelas berdasarkan hasil penilaian risiko.
- b. Memasang alat penggera dan kamera litar tertutup (CCTV).
- c. Mempamerkan papan tanda kawasan larangan.
- d. Menghadkan akses keluar masuk.



- e. Mengadakan kaunter kawalan.
- f. Mewujudkan sistem pas keselamatan.
- g. Mewujudkan perkhidmatan kawalan keselamatan.
- h. Memastikan kawasan dan premis dikawal dari pihak yang tidak berkenaan.

#### **KAWALAN MASUK FIZIKAL**

5. Perkara yang perlu dipatuhi adalah seperti berikut:

- a. Setiap anggota TUDM dan anggota awam hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas.
- b. Semua pas keselamatan hendaklah diserahkan balik kepada TUDM apabila anggota TUDM dan anggota awam berhenti atau bersara.
- c. Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama TUDM dan dikembalikan semula selepas tamat lawatan.
- d. Kehilangan pas mestilah dilaporkan dengan segera mengikut tatacara yang sedang berkuatkuasa di TUDM.
- e. Membuat pemeriksaan mengejut ke atas anggota dan pelawat dari semasa ke semasa.
- f. Menghadkan alatan komunikasi di kawasan yang menempatkan peralatan ICT dan sistem yang mengandungi maklumat sensitif.
- g. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.

**KESELAMATAN PERALATAN**

6. Peralatan ICT hendaklah dijaga dan dikawal dengan baik bagi mengelakkan dari sebarang kehilangan, kerosakan, kecurian atau kompromi ke atas keselamatan aset dan sistem-sistem ICT TUDM. Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

**a. Peralatan ICT.**

- (1) Pengguna hendaklah menyemak dan memastikan semua aset ICT di bawah kawalannya berfungsi dengan baik.
- (2) Pengguna bertanggungjawab sepenuhnya ke atas aset ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan.
- (3) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang aset ICT yang telah ditetapkan tanpa kebenaran BTMK.
- (4) Semua aset ICT hendaklah ditempatkan dan disimpan di tempat yang teratur, bersih dan dilengkapi dengan ciri-ciri keselamatan.
- (5) Setiap pengguna adalah bertanggungjawab di atas kerosakan dan kehilangan aset ICT di bawah jagaannya.
- (6) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini disamping melakukan imbasan ke atas media storan yang digunakan.
- (7) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan.
- (8) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran.

- (9) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS).
- (10) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai.
- (11) Peralatan ICT yang hendak dibawa keluar dari premis TUDM, perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan.
- (12) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera.
- (13) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa.
- (14) Pengguna tidak dibenarkan mengubah kedudukan komputer yang dihubungkan dalam rangkaian dari lokasi asal tanpa kebenaran Pentadbir Sistem ICT.
- (15) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih.
- (16) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal.
- (17) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah kawalannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja.
- (18) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat.



(19) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO.

(20) Memastikan *electrical plug* dicabut daripada suis utama (*main switch*) sebelum meninggalkan pejabat bagi mengelakkan kerosakan perkakasan jika berlaku kejadian seperti petir, kilat dan sebagainya.

**b. Media Storan.**

(1) Media storan merupakan peranti elektronik yang digunakan untuk menyimpan data dan maklumat seperti Disket, Kad multimedia, Pemain MP3, CD, DVD, Pita Magnetik, Cakera Keras, CD-ROM, *Optical Disk*, *Removable Disk* (*External Hard disk/Thumb/Pen Drive*) dan lain-lain.

(2) Keselamatan media storan yang menyimpan maklumat rasmi dan rahsia rasmi Kerajaan perlu diberi perhatian khusus. Langkah-langkah pencegahan hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat.

(3) Semua anggota tentera dan anggota awam dilarang menyimpan maklumat RAHSIA BESAR, RAHSIA, SULIT dan TERHAD di dalam *removable disk* (*External Hard disk/Thumb/Pen Drive*) kecuali dibenarkan oleh pemerintah Markas/Pangkalan/Unit.

(4) Menyediakan ruang penyimpanan khas yang mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat.

(5) Menghadkan capaian kepada pengguna yang dibenarkan sahaja.

(6) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan.

(7) Sebarang pelupusan hendaklah mematuhi tatacara pelupusan.

(8) Mengadakan sistem pengurusan media meliputi inventori, pergerakan, pelabelan dan *backup/restore*.

(9) Semua media hendaklah dilabelkan mengikut tahap kerahsiaan sesuatu maklumat.

(10) Penyelenggaraan media hendaklah dikawal dan direkodkan bagi mengelak dari sebarang kerosakan dan pendedahan maklumat yang tidak dibenarkan.

7. Semua media storan yang mengandungi data berdarjah SULIT dan ke atas hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk kalis daripada api, air, medan-magnet dan tidak boleh dipecahkan.

### **PENYENGGAARAAN PERKAKASAN**

8. Perkakasan hendaklah disenggara dengan betul bagi memastikan kesiagaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut:

- a. Mematuhi manual senggaraan yang ditetapkan oleh pengeluar bagi semua perkakasan yang disenggara.
- b. Memastikan perkakasan hanya disenggara oleh anggota tentera, anggota awam atau pihak yang mempunyai kepakaran dan kelayakan sahaja.
- c. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyenggaraan.
- d. Memaklumkan pihak pengguna sebelum melaksanakan penyenggaraan berjadual yang telah ditetapkan atau atas keperluan.
- e. Semua penyenggaraan mestilah mendapat kebenaran daripada Pengurus ICT/Pentadbir Sistem.

**PENYENGGAHAN PERISIAN DAN APLIKASI**

9. Perisian hendaklah disenggarakan dengan betul bagi memastikan kesiagaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut:

- a. Memastikan perisian baru yang diperolehi perlu melalui ujian penerimaan mengikut piawaian yang ditetapkan.
- b. Memastikan perolehan perisian baru mendapat dokongan teknikal yang berterusan daripada *OEM*.
- c. Memastikan perisian mempunyai lesen yang sah.
- d. Memastikan perisian sentiasa mempunyai versi yang terkini.
- e. Memastikan senggaraan dilaksanakan oleh anggota tentera, anggota awam atau pihak ketiga yang mempunyai kepakaran dan kelayakan sahaja.
- f. Memastikan *source code* yang dibekalkan disimpan ditempat yang selamat.
- g. Memastikan *patch* terkini diuji dan diluluskan oleh pemilik sistem sebelum beroperasi.
- h. Memastikan pemasangan, penambahbaikan dan perubahan perisian yang melibatkan pesawat dilaksanakan oleh pihak yang berkelayakan dan disahkan oleh DJTA.

**PEMINJAMAN PERKAKASAN BAGI KEGUNAAN DI LUAR PEJABAT**

10. Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah perlu diambil termasuklah seperti berikut :

- a. Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh TUDM bagi membawa keluar peralatan, perisian atau maklumat tertakluk kepada tujuan yang dibenarkan.



- b. Melindungi dan mengawal peralatan sepanjang masa.
- c. Merekod aktiviti peminjaman dan pemulangan peralatan.
- d. Memastikan peralatan yang dipulangkan berada dalam keadaan baik.

### **PENGENDALIAN PERALATAN LUAR YANG DIBAWA MASUK/KELUAR**

11. Bagi peralatan yang dibawa masuk/keluar ke TUDM, langkah keselamatan yang perlu diambil adalah seperti berikut:
- a. Memastikan peralatan yang dibawa masuk/keluar tidak mengancam keselamatan ICT TUDM.
  - b. Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh TUDM bagi membawa masuk/keluar peralatan.
  - c. Memastikan peralatan yang mempunyai maklumat berdarjah yang dibawa keluar daripada TUDM diawasi pada sebilang masa.

### **PELUPUSAN ASET**

12. Pelupusan melibatkan semua aset ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dimiliki oleh TUDM perlu mematuhi tatacara yang ditetapkan. Proses pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan TUDM. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:
- a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding*, *grinding*, *degauzing* atau pembakaran. Pengguna dibenarkan membuat salinan pendua sekiranya maklumat perlu disimpan untuk rujukan masa hadapan.

- b. Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat.
- c. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya.
- d. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut.
- e. Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset.
- f. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuatkuasa di TUDM.
- g. Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:
  - (1) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya.
  - (2) Menyimpan dan memindahkan aksesori komputer yang masih boleh digunakan seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di TUDM.
  - (3) Memindah keluar dari TUDM mana-mana peralatan ICT yang hendak dilupuskan.
  - (4) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan adalah di bawah tanggungjawab TUDM.

### **KESELAMATAN PERSEKITARAN**

- 13. Melindungi aset ICT Kerajaan dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesusilaan, kecuriahan atau kemalangan.

14. **Kawalan Persekitaran** . Menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan perolehan dan pengubahsuaian hendaklah dirujuk terlebih dahulu kepada BTMK. Perkara yang perlu dipatuhi adalah seperti berikut:

- a. Merancang dan menyediakan pelan keseluruhan pusat data termasuk ruang peralatan komputer, ruang percetakan dan ruang atur pejabat.
- b. Melengkapi semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT dengan perlindungan keselamatan yang bersesuaian.
- c. Memasang peralatan perlindungan di tempat yang bersesuaian, mudah dikenali dan dikendalikan.
- d. Menyimpan/meletak bahan mudah terbakar dan bahan cecair di luar kawasan penyimpanan aset ICT.
- e. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer.
- f. Menyemak dan menguji semua peralatan perlindungan sekurang-kurangnya dua (2) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.
- g. Menetapkan suhu premis mengikut spesifikasi perkakasan yang diperlukan.

15. **Bekalan Kuasa**. Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara yang perlu dipatuhi bagi menjamin keselamatan bekalan kuasa adalah seperti berikut:

- a. Melindungi semua peralatan ICT dari bekalan elektrik yang tidak stabil dan menyalurkan bekalan yang sesuai kepada peralatan ICT.
- b. Menggunakan peralatan sokongan seperti UPS (*Uninterruptible Power Supply*) dan penjana elektrik (*generator*) bagi perkhidmatan kritikal seperti di bilik *server* supaya mendapat bekalan kuasa berterusan.



- c. Memeriksa dan menguji semua peralatan sokongan bekalan kuasa secara berjadual.

16. **Keselamatan Kabel.** Kabel elektrik dan telekomunikasi yang menyalurkan data atau menyokong sistem penyampaian perkhidmatan hendaklah dilindungi daripada pencerobohan dan kerosakan. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:

- a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan.
- b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan.
- c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*.
- d. Memastikan kabel dilabelkan dengan kod tertentu.

17. **Prosedur Kecemasan.** Perkara yang perlu dipatuhi bagi memastikan keselamatan aset ICT adalah seperti berikut:

- a. Memastikan setiap pengguna membaca, memahami dan mematuhi prosedur kecemasan yang ditetapkan oleh Pegawai Keselamatan yang dilantik.
- b. Melaporkan insiden kecemasan persekitaran seperti kebakaran kepada Pegawai Keselamatan yang dilantik.
- c. Mengadakan, menguji dan mengemaskini pelan kecemasan dari semasa ke semasa.
- d. Mengadakan latihan *fire drill* mengikut jadual.

**KESELAMATAN DOKUMEN**

18. Melindungi maklumat TUDM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuai. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a. Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti TERBUKA, TERHAD, SULIT, RAHSIA atau RAHSIA BESAR.
- b. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur Arahan Keselamatan.
- c. Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan.
- d. Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara.
- e. Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.

**CLEAR DESK DAN CLEAR SCREEN**

19. Prosedur *Clear Desk* dan *Clear Screen* perlu dipatuhi supaya maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Perkara yang perlu dipatuhi adalah seperti berikut:

- a. Menggunakan kemudahan kata laluan *screen saver* apabila meninggalkan komputer.
- b. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci.
- c. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.

**MANUAL PENGURUSAN KESELAMATAN ICT TUDM**

**BAHAGIAN 3**



**MANUAL PENGURUSAN KESELAMATAN ICT TUDM****BAHAGIAN 3****RISALAH 1****PENGURUSAN OPERASI DAN KOMUNIKASI****PENDAHULUAN**

1. Prosedur pengurusan operasi dan komunikasi hendaklah didokumenkan, disenggarakan dan mudah didapati apabila diperlukan.

**TUJUAN**

2. Memastikan pengurusan operasi dan komunikasi berfungsi dengan baik dan selamat dari sebarang ancaman atau gangguan.

**PENGURUSAN OPERASI DAN KOMUNIKASI**

3. Markas/Pangkalan/Unit yang memiliki sistem ICT masing-masing adalah bertanggungjawab untuk memastikan kesemua kemudahan pemprosesan maklumat adalah terjamin selamat dan berjalan lancar.

**TANGGUNGJAWAB DAN PROSEDUR OPERASI**

4. Bagi memastikan kemudahan pemprosesan maklumat berfungsi seperti yang ditetapkan, Markas/Pangkalan/Unit bertanggungjawab menentukan perkara berikut dipatuhi:
  - a. Semua prosedur operasi hendaklah didokumenkan dengan jelas lagi teratur, dikemaskini dan sedia digunakan oleh pengguna mengikut keperluan.
  - b. Setiap perubahan kepada sistem dan kemudahan pemprosesan maklumat mestilah dikawal.
  - c. Tugas dan tanggungjawab perlu diasingkan bagi mengurangkan risiko kecuaiian dan penyalahgunaan aset ICT TUDM.
  - d. Peralatan ICT untuk pembangunan, pengujian dan operasi mestilah diasingkan bagi mengurangkan risiko capaian atau pengubahsuaian secara tidak sah ke atas sistem yang sedang beroperasi.

**PENGURUSAN PENYAMPAIAN PERKHIDMATAN PEMBEKAL, PAKAR RUNDING DAN  
PIHAK-PIHAK LAIN YANG TERLIBAT**

5. Bagi memastikan pelaksanaan dan penyenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pembekal, pakar runding dan pihak-pihak lain yang terlibat, perkara-perkara yang mesti dipatuhi adalah seperti berikut:

- a. Memastikan kawalan keselamatan, definasi perkhidmatan dan tahap penyampaian (*Service Level Agreement*) yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat.
- b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa.
- c. Pengurusan ke atas perubahan penyediaan perkhidmatan termasuk menyenggara dan menambah baik polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.

**PERANCANGAN DAN PENERIMAAN SISTEM**

6. Bagi mengurangkan risiko yang menyebabkan gangguan atau kegagalan sistem, perkara-perkara yang mesti dipatuhi adalah seperti berikut:

- a. Perancangan perlu dibuat bagi memenuhi keperluan kapasiti akan datang untuk memastikan prestasi sistem di tahap optimum.
- b. Kriteria penerimaan untuk peralatan dan sistem baru, peningkatan dan versi baru perlu ditetapkan dan ujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem.
- c. Pelan ujian penerimaan dan senarai semak perlu disediakan dan dipatuhi setiap kali perolehan baru aset ICT TUDM.



**PERLINDUNGAN DARI MALICIOUS CODE**

7. Melindungi integriti maklumat dan perisian dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti *virus*, *worm*, *trojan* dan lain-lain. Perkara-perkara yang mesti dipatuhi adalah seperti berikut:

- a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) dan mengikut prosedur penggunaan yang selamat.
- b. Memasang dan menggunakan hanya perisian yang tulen.
- c. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.
- d. Mengemaskini perisian antivirus dari semasa ke semasa.
- e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan atau kerosakan maklumat.
- f. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengatasinya.
- g. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya.
- h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan.
- i. Memberi amaran mengenai ancaman seperti serangan virus terhadap keselamatan aset ICT TUDM.
- j. Melaksanakan kawalan pencegahan, pengesanan dan pemulihan untuk melindungi daripada *malicious code*.
- k. Dalam keadaan di mana *mobile code* dibenarkan, konfigurasi mestilah dipastikan ianya beroperasi berdasarkan kepada manual keselamatan. Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.
- l. Memastikan komputer peribadi yang mempunyai capaian Internet ditutup apabila tidak digunakan.



**BACKUP (SALINAN PENDUA)**

8. Salinan pendua hendaklah direkodkan dan disimpan di lokasi yang berlainan (*off site*). Perkara yang mesti dipatuhi adalah seperti berikut:

- a. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru.
- b. Membuat salinan pendua ke atas semua data dan maklumat mengikut kesesuaian operasi.
- c. Menguji sistem pendua sedia ada secara berkala bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan supaya dapat digunakan apabila diperlukan khususnya pada waktu kecemasan.
- d. Salinan pendua perlu dilaksanakan terlebih dahulu sebelum penambahbaikan aset ICT dilakukan.

**PENGURUSAN KESELAMATAN RANGKAIAN**

9. Memastikan perlindungan keselamatan maklumat dalam rangkaian dan infrastruktur sokongan terus dan terkawal. Infrastruktur rangkaian mestilah dikawal, dipantau dan diurus sebaiknya, demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- a. Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem rangkaian.
- b. Ciri-ciri keselamatan, tahap perkhidmatan dan keperluan pengurusan bagi semua perkhidmatan rangkaian perlu dikenal pasti dan dimasukkan dalam mana-mana perjanjian perkhidmatan rangkaian sama ada perkhidmatan berkenaan disediakan secara dalaman atau melalui khidmat luar.
- c. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan.
- d. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko kerosakan seperti banjir, gegaran, habuk dan lain-lain.

- e. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja.
- f. *Firewall* hendaklah dipasang di antara rangkaian dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh pentadbir sistem yang dibenarkan sahaja.
- g. Semua *traffic* keluar dan masuk hendaklah melalui *firewall* di bawah kawalan TUDM.
- h. Semua perisian *sniffer* atau *network analyzer* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO.
- i. Memasang perisian *Intrusion Detection System (IDS)* dan *Intrusion Prevention System (IPS)* bagi mengesan sebarang cubaan mencerooboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat TUDM.
- j. Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam PKPA 1/2003.
- k. Sebarang penyambungan rangkaian yang bukan di bawah kawalan TUDM adalah tidak dibenarkan. Keperluan rangkaian baru perlu dimohon kepada BTMK.
- l. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang optimum.
- m. Penggunaan rangkaian tanpa wayar (*wireless*) LAN di TUDM hendaklah mematuhi surat KEMENTAH dengan rujukan UPTM (S) 159/338/8 Jilid 30 (84) bertajuk "Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) Di Agensi-agensi Kerajaan".

### **POLISI DAN PROSEDUR PERTUKARAN MAKLUMAT**

- 10. Memastikan perlindungan keselamatan maklumat dalam rangkaian dan infrastruktur sokongan terurus dan terkawal. Perkara yang perlu dipatuhi adalah seperti berikut :



- a. Polisi, prosedur dan kawalan rangkaian TUDM yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi.
- b. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari Markas/Pangkalan/Unit TUDM.
- c. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.

#### PERKHIDMATAN MEL ELEKTRONIK (E-MEL)

11. Maklumat yang terdapat dalam e-mel TUDM perlu dilindungi sebaik-baiknya bagi menghindari capaian atau sebaran maklumat yang tidak dibenarkan. Semua anggota TUDM dan anggota awam layak menerima kemudahan perkhidmatan e-mel mengikut keperluan tugas dan perlu mendapat kelulusan dari pemerintah Markas/Pangkalan/Unit. Perkara yang perlu dipatuhi adalah seperti berikut:

- a. Etika Penggunaan Internet Dan E-mel TUDM perlu dipatuhi oleh semua pengguna TUDM selaras dengan Perintah Am Angkatan Tentera Bahagian IX – Bahagian Perisikan Pertahanan, Perintah Pencegahan Pencemaran Maklumat ATM Melalui Platform Siber, Bilangan 1/2013 bertarikh 11 Jan 13.
- b. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh TUDM/MINDEF adalah untuk kegunaan rasmi sahaja. Penggunaan *free web-based mail* untuk kegunaan rasmi **DILARANG** sama sekali. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang.
- c. Segala akaun e-mel yang diberi adalah bukan hak persendirian.
- d. Pentadbir Sistem e-mel berhak mengakses atas sebab-sebab tertentu untuk tujuan keselamatan dan undang-undang.
- e. Setiap e-mel yang disediakan hendaklah mematuhi format yang ditetapkan oleh TUDM.
- f. Sebarang penggunaan yang boleh memudaratkan nama baik TUDM adalah dilarang sama sekali.



- g. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan.
- h. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui.
- i. Pengguna hendaklah mengenalpasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel.
- j. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan.
- k. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan.
- l. Pentadbir e-mel hendaklah menentukan tarikh dan masa sistem komputer adalah tepat.
- m. Maklumat yang terdapat dalam e-mel perlu dilindungi dengan baik.
- n. Setiap e-mel yang berdarjah hendaklah dienkrif terlebih dahulu sebelum dihantar.

### **TELECOMMUTING**

12. Memastikan keselamatan maklumat yang diakses atau dihantar semasa menggunakan kemudahan *telecommuting* adalah terjamin. Perkara yang perlu dipatuhi adalah seperti berikut:
- a. Kemudahan ini disediakan hanya untuk sistem-sistem yang dibenarkan sahaja.
  - b. Kebenaran untuk menggunakan perkhidmatan hendaklah diberikan secara bertulis oleh Pengurus Sistem dengan menggunakan komputer peribadi perkhidmatan sahaja.

c. Sistem yang diakses dari luar hendaklah mempunyai sistem enkripsi (*encryption*) yang mencukupi. Menghantar kata laluan tanpa enkripsi adalah dilarang sama sekali.

d. Individu yang dibenarkan untuk menggunakan kemudahan ini adalah bertanggungjawab sepenuhnya ke atas peralatan dan data sepanjang melakukan tugasnya. Sekiranya individu ini terpaksa menghantar maklumat berdarjah ia mestilah menggunakan enkripsi yang dibenarkan oleh TUDM.

### **KOMUNIKASI TANPA WAYAR (WIRELESS)**

13. Polisi ini merangkumi semua peranti perhubungan data tanpa wayar (komputer peribadi, telefon selular, PDA dan sebagainya) yang bersambung dengan sebarang rangkaian dalaman TUDM. Ia termasuklah sebarang bentuk peranti komunikasi tanpa wayar yang berupaya menghantar paket data. Peranti dan/atau rangkaian tanpa wayar tanpa sebarang sambungan ke rangkaian TUDM tidak tertakluk kepada polisi ini. Berikut ialah polisi yang berkaitan dengan komunikasi tanpa wayar.

a. Titik Capaian Berdaftar. Titik Capaian (*Access Point*) tidak dibenarkan disambungkan ke rangkaian sistem ICT. Penggunaan titik capaian perlu mendapat kelulusan bertulis dari BTMK (sekiranya talian tetap tidak dapat disediakan).

b. Teknologi Yang Diperakui. Semua capaian LAN tanpa wayar mesti menggunakan produk dan konfigurasi keselamatan dari vendor yang diperakui.

c. Virtual Private Network (VPN). Semua komputer dengan peranti LAN tanpa wayar mesti menggunakan konfigurasi VPN yang diperakui untuk mengelak trafik yang tidak berautentikasi dan tidak dienkrip. Untuk mematuhi polisi ini, pelaksana tanpa wayar mesti mematuhi enkripsi *point to point* yang ditetapkan oleh TUDM. Semua peralatan mesti disokong oleh alamat perkakasan yang boleh didaftar dan dikesan kembali (seperti alamat MAC).

d. Melaraskan Service Set Identifier (SSID). SSID mesti dikonfigurasi supaya ia tidak mempunyai sebarang maklumat pengenalan berkenaan dengan organisasi, seperti nama organisasi, nama bahagian, nama staf atau pengenalan produk.



**BRING YOUR OWN DEVICE (BYOD)**

14. BYOD adalah peralatan mudah alih persendirian seperti telefon pintar, *tablet*, dan *lapotop* yang digunakan untuk tujuan rasmi. Maklumat lanjut mengenai BYOD boleh dirujuk Polisi Berkaitan ***Bring Your Own Device (BYOD)*** seperti di **KEMBARAN C Dasar Keselamatan ICT MINDEF Versi 4.0**.

**PENGENDALIAN MEDIA**

15. Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan. Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut:

- a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat.
- b. Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja.
- c. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja.
- d. Mengawal dan merekodkan aktiviti penyenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan.
- e. Menyimpan semua media yang mengandungi maklumat yang dibenarkan dan versi terkini sahaja di tempat yang selamat.
- f. Media yang mengandungi maklumat berdarjah yang hendak dihapuskan, dimusnahkan atau dilupuskan mesti mengikut prosedur yang betul dan selamat.

**PROSEDUR PENGENDALIAN MAKLUMAT**

16. Prosedur ini bertujuan untuk mengendali, menyimpan, memindah serta melindungi maklumat daripada didedah tanpa kebenaran atau salah guna. Memastikan keselamatan pertukaran maklumat dan mana-mana entiti luar terjamin. Perkara yang perlu dipatuhi adalah seperti berikut:

- a. Menghadkan dan menentukan capaian kepada pengguna yang dibenarkan sahaja.



- b. Menghadkan pengedaran data untuk tujuan rasmi dan yang dibenarkan sahaja.
- c. Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi.
- d. Sebarang pertukaran maklumat di antara TUDM dan agensi kerajaan yang lain mestilah dikawal dan direkod.
- e. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara TUDM dengan pihak luar.
- f. Pengendalian maklumat melalui internet hendaklah selaras dengan Perintah Am Angkatan Tentera Bahagian IX – Bahagian Perisikan Pertahanan, Perintah Pencegahan Pencemaran Maklumat ATM Melalui Platform Siber, Bilangan 1/2013 bertarikh 11 Jan 13.

#### **KESELAMATAN SISTEM DOKUMENTASI**

17. Sistem dokumentasi perlu dilindungi dari capaian yang tidak dibenarkan. Langkah-langkah pengurusan dokumentasi yang baik dan selamat perlu dilaksanakan bagi memastikan integriti maklumat. Perkara yang perlu dipatuhi adalah seperti berikut:
- a. Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin.
  - b. Menggunakan tanda atau label keselamatan seperti RAHSIA BESAR, RAHSIA, SULIT atau TERHAD pada dokumen.
  - c. Mewujudkan sistem pengurusan dokumen berdarjah bagi menerima, memproses, menyimpan dan menghantar dokumen-dokumen tersebut supaya ianya diuruskan berasingan daripada dokumen-dokumen tidak berdarjah.
  - d. Menggunakan enkripsi ke atas dokumen berdarjah yang disediakan dan dihantar secara elektronik.

- e. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.

### **PENGAUDITAN DAN FORENSIK ICT**

18. ICTSO hendaklah memastikan semua proses pengauditan dan forensik ICT dijalankan bagi menjamin keselamatan ICT sentiasa terpelihara. Pentadbir sistem hendaklah merekod dan menganalisis perkara-perkara berikut:

- a. Sebarang percubaan pencerobohan kepada sistem ICT TUDM.
- b. Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*).
- c. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak.
- d. Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan.
- e. Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan.
- f. Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian.
- g. Aktiviti penyalahgunaan akaun e-mel.
- h. Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT TUDM.

### **JEJAK AUDIT**

19. Setiap sistem mestilah mempunyai jejak audit. Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula sesuatu kejadian mengikut susunan dan perubahan. Jejak audit hendaklah mengandungi maklumat-maklumat berikut:

- a. Rekod setiap aktiviti transaksi.
- b. Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan.
- c. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya.
- d. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.
- e. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara.
- f. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal.
- g. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.

### **SISTEM LOG**

20. Setiap sistem semestinya mempunyai sistem log. Sistem log merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan mengikut susunan dan perubahan dalam sesuatu acara. Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:

- a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian.
- b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaikpulih dengan segera.



c. Sekiranya wujud aktiviti-aktiviti yang diragui atau tidak sah di mana boleh memudaratkan perkhidmatan, hendaklah dilaporkan kepada TUDM\*CERT dengan segera.

### **PEMANTAUAN LOG**

21. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian.
- b. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala.
- c. Maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan.
- d. Aktiviti pentadbiran dan operator sistem perlu direkodkan.
- e. Kesalahan, kesilapan, dan penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya.
- f. Waktu yang berkaitan dengan sistem pemprosesan maklumat TUDM atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.
- g. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera.
- h. Sekiranya wujud aktiviti-aktiviti tidak sah seperti kecurian maklumat dan pencerobohan hendaklah dilaporkan kepada TUDM\*CERT.

**MANUAL PENGURUSAN KESELAMATAN ICT TUDM****BAHAGIAN 3****RISALAH 2****KAWALAN CAPAIAN****PENDAHULUAN**

1. Peraturan kawalan capaian hendaklah diwujudkan, didokumen dan dikaji semula berasaskan keperluan pengurusan TUDM dan keselamatan.

**TUJUAN**

2. Melindungi maklumat dari sebarang bentuk capaian yang dilakukan tanpa kebenaran.

**KAWALAN CAPAIAN**

3. Mengawal capaian ke atas maklumat, kemudahan proses maklumat dan proses kerja berdasarkan keperluan dan keselamatan. Peraturan kawalan capaian hendaklah mengambil kira faktor *identification*, *authentication* dan *authorization*.

**DASAR KAWALAN CAPAIAN**

4. Perkara yang perlu dipatuhi adalah seperti berikut :
  - a. Kawalan capaian ke atas maklumat dan proses mengikut keperluan keselamatan dan peranan pengguna.
  - b. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran.
  - c. Kawalan capaian ke atas kemudahan pemprosesan maklumat oleh pengguna.
  - d. Keselamatan bagi maklumat yang dicapai menggunakan peralatan mudah alih.
  - e. Memastikan bahawa sistem maklumat hanya dicapai oleh pengguna yang sah.

5. Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna. Setiap capaian perlu direkod, dikemaskini dan hendaklah mematuhi dasar capaian pengguna yang berkuatkuasa.

### **PENGURUSAN CAPAIAN PENGGUNA**

6. Pengurusan capaian adalah merujuk kepada kawalan capaian ke atas sistem pengoperasian, aplikasi dan maklumat melalui rangkaian TUDM bagi memastikan bahawa sistem hanya dicapai oleh pengguna yang sah. Perkara yang perlu dipatuhi adalah seperti berikut:

- a. Memastikan bahawa sistem maklumat dicapai oleh pengguna yang sah dan menghalang capaian yang tidak sah.
- b. Prosedur yang melibatkan proses pendaftaran dan pembatalan kebenaran capaian pengguna perlu diwujudkan dan didokumenkan.
- c. Aktiviti capaian pengguna direkod dan dikaji secara berkala. Maklumat yang direkod termasuk identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh, masa, rangkaian dilalui, aplikasi diguna dan aktiviti capaian secara sah atau sebaliknya.

### **PENDAFTARAN DAN PEMBATALAN AKAUN**

7. Prosedur pendaftaran dan pembatalan kebenaran capaian pengguna perlu diwujudkan dan didokumenkan. Perkara yang perlu dipatuhi adalah seperti berikut:

- a. Akaun pengguna adalah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat.
- b. Akaun pengguna yang diwujudkan dan tahap capaian termasuk sebarang perubahan mestilah mendapat kebenaran pemerintah Markas/Pangkalan/Unit secara bertulis dan direkodkan.
- c. Pemilihan akaun dan capaian pengguna adalah tertakluk kepada peraturan Markas/Pangkalan/Unit dan tindakan pembatalan/pengubahsuaian hendaklah diambil atas sebab seperti berikut:



- (1) Pengguna tidak hadir bertugas tanpa kebenaran melebihi satu tempoh yang ditentukan oleh pemerintah Markas/Pangkalan/Unit.
- (2) Pengguna bercuti atau bertugas di luar pejabat.
- (3) Melebihi satu tempoh yang ditentukan oleh pemerintah Markas/Pangkalan/Unit.
- (4) Pengguna bertukar jawatan, tanggungjawab dan/atau bidang tugas.
- (5) Pengguna bertukar keluar atau berpindah.
- (6) Pengguna bersara atau tamat perkhidmatan.

#### **HAK CAPAIAN (PRIVILEGE)**

8. Penetapan dan penggunaan ke atas capaian memerlukan kawalan dan seliaan yang ketat. Hak capaian hendaklah sentiasa dipantau dan dikemaskini mengikut keperluan semasa. Prosedur yang melibatkan proses kawalan capaian perlu diwujudkan dan didokumenkan.

#### **PENGURUSAN KATA LALUAN**

9. Pemilihan, penggunaan dan pengurusan kata laluan bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh TUDM seperti berikut:

- a. Kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun.
- b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya pencerobohan kata laluan atau dikompromi.
- c. Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun.
- d. Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama.
- e. Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program.

- f. Penguatkuasaan pertukaran kata laluan semasa *login* kali pertama atau selepas kata laluan diperbaharui.
- g. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna.
- h. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian.
- i. Mengelakkan penggunaan semula kata laluan yang pernah digunakan.

#### **POLISI CLEAR DESK AND CLEAR SCREEN**

10. *Clear desk and clear screen* bermaksud tidak meninggalkan bahan-bahan sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci.
- b. Menggunakan kemudahan *password screen saver* atau *logout / lock* apabila meninggalkan komputer.
- c. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.

#### **KAWALAN CAPAIAN RANGKAIAN**

11. Menghalang capaian tidak sah dan tanpa kebenaran ke atas rangkaian TUDM. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

- a. Menempatkan atau memasang antaramuka yang menepati kesesuaian penggunaannya di antara rangkaian TUDM dan rangkaian lain-lain organisasi.
- b. Mewujudkan dan menguatkuasakan mekanisma untuk pengesanan pengguna dan peralatan yang menepati kesesuaian penggunaannya.
- c. Mewujudkan segmen rangkaian yang bersesuaian bagi membezakan had capaian pengguna dan keperluan sistem.



- d. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.
- e. Mewujudkan mekanisme pengesahan yang sesuai untuk mengawal capaian oleh pengguna jarak jauh.
- f. Capaian fizikal dan logikal ke atas perkakasan rangkaian bagi tujuan mengubah konfigurasi perlulah dikawal.
- g. Memastikan pengguna boleh mencapai perkhidmatan yang dibenarkan sahaja.
- h. Mewujudkan mekanisma pengesahan yang sesuai untuk mengawal capaian oleh pengguna jarak jauh.
- i. Menggunakan kaedah pengenalan automatik berdasarkan lokasi dan peralatan untuk pengesahan sambungan ke dalam rangkaian.
- j. Mengawal capaian fizikal dan logikal ke atas kemudahan *diagnostic port* dan konfigurasi jarak jauh.
- k. Mengasingkan capaian mengikut kumpulan perkhidmatan, maklumat pengguna dan sistem maklumat dalam rangkaian.
- l. Mengawal sambungan ke rangkaian, khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan TUDM.
- m. Mewujud dan melaksanakan kawalan pengalihan laluan (*routing control*) untuk memastikan pematuhan ke atas peraturan TUDM.

#### **PERKHIDMATAN INTERNET**

12. Capaian Internet perlu dikawal dan diurus bagi mengelakkan gangguan sistem rangkaian TUDM. Perkara yang perlu dipatuhi adalah seperti berikut :

- a. Pengguna Internet di setiap Markas/Pangkalan/Unit TUDM hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaan hanya untuk tujuan yang dibenarkan sahaja
- b. Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan.



- c. Melayari laman web yang menentang pemerintahan kerajaan, berunsur hasutan dan mempunyai unsur-unsur lucah yang boleh menjatuhkan imej TUDM adalah DILARANG sama sekali.
- d. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan.
- e. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada pemerintah Markas/Pangkalan/Unit sebelum dimuat naik ke Internet.
- f. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hakcipta terpelihara.
- g. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh TUDM.
- h. Pengurusan *bandwidth* hendaklah digunakan untuk mengawal aktiviti seperti *video conferencing*; *video streaming*, *chat*, *downloading* bagi mengawal penggunaan *bandwidth* mengikut keperluan.
- i. Arahan yang dikeluarkan mengenai “Etika Penggunaan Internet dan E-mel Kementerian Pertahanan” seperti di Kembaran B Dasar Keselamatan ICT MinDef dan Perintah Am Angkatan Tentera Bahagian IX – Bahagian Perisikan Pertahanan, Perintah Pencegahan Pencemaran Maklumat ATM Melalui Platform Siber, Bilangan 1/2013 bertarikh 11 Jan 13 perlu dipatuhi oleh semua pengguna TUDM.

#### **KAWALAN CAPAIAN SISTEM PENGOPERASIAN**

13. Memastikan bahawa capaian ke atas sistem pengoperasian dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. Kaedah yang digunakan hendaklah menyokong perkara-perkara berikut:
- a. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan TUDM.
  - b. Mewujudkan jejak audit ke atas semua capaian sistem operasi terutama pengguna bertaraf khas (*super user*).
  - c. Menjana amaran (*alert*) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem.

- d. Menyedia kaedah sesuai untuk pengesahan capaian (*authentication*).
  - e. Menghadkan tempoh penggunaan mengikut kesesuaian.
14. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log-in* yang selamat. Prosedur *log-in* yang selamat perlulah:
- a. Menggunakan kaedah pengenalan pengguna yang unik dan teknik pengesahan pengguna yang berkesan dan selamat.
  - b. Melaksanakan sistem pengurusan kata laluan yang interaktif dan menjamin kualiti serta keselamatan kata laluan.
  - c. Mengawal penggunaan utiliti yang berkeupayaan melepasi sistem dan aplikasi terhad.
  - d. Menamatkan sesi yang tidak aktif selepas tempoh masa yang ditetapkan.
  - e. Hadkan tempoh masa penggunaan bagi meningkatkan keselamatan aplikasi yang berisiko tinggi.

#### **KAWALAN CAPAIAN APLIKASI DAN MAKLUMAT**

15. Menghalang capaian tidak sah ke atas sistem aplikasi dan maklumat. Perkara-perkara yang perlu dipatuhi ialah :
- a. Membenarkan pengguna mencapai aplikasi dan maklumat mengikut tahap capaian yang ditentukan.
  - b. Menyediakan mekanisme perlindungan bagi menghalang capaian yang tidak sah ke atas aplikasi dan maklumat daripada utiliti yang sedia ada dalam sistem operasi dan perisian *malicious* yang berupaya melangkaui kawalan sistem.
  - c. Mengawal dan menghadkan sebarang sistem yang berkongsi data secara terus, dengan menggunakan sistem pengantara bagi membolehkan perkongsian data.
  - d. Capaian ke atas maklumat dan fungsi sistem aplikasi oleh pengguna perlu dihadkan selaras dengan peraturan TUDM.



- e. Sistem yang sensitif memerlukan persekitaran pengkomputeran yang khusus dan terasing.
- f. Setiap aktiviti capaian pengguna ke atas aplikasi dan maklumat hendaklah direkod (sistem log).
- g. Capaian aplikasi dan maklumat melalui jarak jauh adalah digalakkan. Walau bagaimanapun penggunaannya hendaklah dihadkan kepada perkhidmatan yang dibenarkan sahaja.

### **CAPAIAN JARAK JAUH**

16. Capaian jarak jauh adalah merujuk kepada capaian daripada sistem rangkaian dalaman dan daripada sistem rangkaian luaran bagi lokasi luar pejabat untuk tujuan *telecommuting* yang perlu dikawal bagi memastikan keselamatan. Perkara-perkara yang perlu dipatuhi ialah:

- a. Penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi.
- b. Lokasi bagi akses ke sistem ICT TUDM hendaklah dipastikan selamat.
- c. Penggunaan perkhidmatan jarak jauh hendaklah mendapat kebenaran daripada Pengurus ICT TUDM.
- d. Pengguna yang diberi hak adalah bertanggungjawab sepenuhnya ke atas penggunaan kemudahan yang diberikan.

### **PERALATAN MUDAH ALIH**

17. Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih (telefon pintar, *tablet* dan *laptop*). Perkara yang perlu dipatuhi adalah seperti berikut:

- a. Pengguna bertanggungjawab menentukan maklumat berdarjah dan ia perlu melalui proses enkripsi yang dibenarkan sebelum dihantar atau disalurkan ke dalam sistem rangkaian yang tidak selamat (seperti Internet, Mobil-GSM, Infrared, Bluetooth, WAP, 3G, NFC dan sebagainya).



b. Bagi pengguna peralatan mudah alih yang dibekalkan oleh kerajaan perlu mematuhi perkara-perkara berikut:

- (1) Merekod aktiviti keluar masuk penggunaan peralatan mudah alih bagi mengesan pergerakan perkakasan tersebut daripada kehilangan atau kerosakan.
- (2) Peralatan mudah alih hendaklah disimpan atau dikunci di tempat yang selamat apabila tidak digunakan.
- (3) Memastikan peralatan mudah alih yang dibawa keluar dari pejabat perlu disimpan dan dijaga dengan baik bagi mengelakkan daripada kecurian.

c. Bagi peralatan mudah alih persendirian, pengguna dikehendaki merujuk Polisi Berkaitan *Bring Your Own Device (BYOD)* di Kembaran C DKICT MINDEF.

**MANUAL PENGURUSAN KESELAMATAN ICT TUDM****BAHAGIAN 3****RISALAH 3****PEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM****PENDAHULUAN**

1. Perolehan, pembangunan, dan penyenggaraan sistem sedia ada atau sistem baru hendaklah mengambilkira keperluan-keperluan kawalan keselamatan.

**TUJUAN**

2. Memastikan aspek keselamatan dikenalpasti dan diambilkira dalam semua sistem termasuk sistem pengoperasian, infrastruktur, sistem aplikasi dan perisian.

**KEPERLUAN KESELAMATAN SISTEM**

3. Perkara-perkara yang perlu dilaksanakan dan dipatuhi adalah seperti berikut:
  - a. Memastikan bahawa aspek keselamatan dikenalpasti, dipersetujui dan didokumenkan pada setiap peringkat perolehan, pembangunan dan penyenggaraan.
  - b. Penyataan keperluan bagi sistem baru atau penambahbaikan ke atas sistem sedia ada hendaklah menjelaskan mengenai kawalan jaminan keselamatan.

**PENGESAHAN DATA INPUT DAN OUTPUT**

4. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:
  - a. Data *input* bagi sistem perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian.
  - b. Data *output* daripada sistem perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.

**KAWALAN KRIPTOGRAFI**

5. Memastikan kaedah kriptografi digunakan untuk melindungi kerahsiaan, kesahihan dan integriti maklumat melalui teknik kriptografi. Perkara yang perlu dipatuhi adalah seperti berikut:

- a. Penggunaan enkripsi ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.
- b. Penggunaan tandatangan digital kepada semua pengguna yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.
- c. Pengurusan kekunci (*key management*) dilakukan dengan berkesan dan selamat bagi melindungi kekunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kekunci tersebut.

#### **KESELAMATAN FAIL SISTEM DAN KOD SUMBER PROGRAM**

6. Memastikan capaian ke atas fail-fail sistem dan kod sumber program adalah terkawal dan aktiviti-aktiviti sokongan dilaksanakan dalam keadaan yang selamat. Kawalan perlu diambil untuk mengelakkan pendedahan maklumat sensitif semasa proses pengujian dilaksanakan. Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut:

- a. Mewujudkan peraturan yang mengawal pemasangan perisian ke dalam sistem yang sedang beroperasi.
- b. Melindungi dan mengawal fail sistem, kod sumber dan data-data ujian.
- c. Menghadkan capaian ke atas kod sumber program kepada pengguna yang dibenarkan sahaja.

#### **KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN**

7. Bagi memastikan keselamatan perisian sistem aplikasi dan maklumat dikawal supaya selamat dalam semua keadaan, perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a. Mengawal pelaksanaan perubahan menggunakan prosedur kawalan perubahan yang formal.
- b. Mengkaji semula dan menguji aplikasi kritikal semasa melaksanakan perubahan ke atas sistem yang sedang beroperasi untuk memastikan tiada impak negatif ke atas keselamatan operasi dan latihan TUDM.
- c. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja.



- d. Menghalang sebarang percubaan membocorkan maklumat.
- e. Mengawal selia dan membantu pembangunan perisian oleh pembekal, pakar perunding dan pihak-pihak lain yang terlibat.
- f. Mengesahkan segala perubahan dan/atau pindaan ke atas sistem yang sedang beroperasi dan/atau pakej perisian sebelum diguna pakai.
- g. Sesuatu sistem yang tidak diguna pakai hendaklah melalui proses pembersihan data yang sedia ada sebelum ianya dilupuskan.

### **PEMBANGUNAN PERISIAN SECARA *OUTSOURCE***

8. *Outsourcing* merujuk kepada perkhidmatan pengurusan sebahagian atau keseluruhan sistem ICT oleh pihak ketiga. *Outsourcing* ini boleh membantu penggunaan ICT dalam keadaan kekurangan staf dan kemahiran. Namun begitu, pada masa yang sama ia dapat memudahkan maklumat diperolehi oleh kontraktor atau pembekal yang dilantik. Bagi menjamin keselamatan sistem, perkhidmatan *outsourcing* perlu dikawal. Kod sumber program bagi semua aplikasi dan perisian adalah menjadi hak milik TUDM.

### **DASAR PELAKSANAAN *OUTSOURCING***

- 9. Semua kontraktor yang melaksanakan perkhidmatan *outsourcing* mesti melepasi tapisan keselamatan. Maklumat berdarjah hendaklah dimaklumkan secara *need to know basis*. Ianya dapat dilaksanakan dengan mengawal tahap akses kebenaran keselamatan (*security level access clearance*).
- 10. Tim penilaian atau pakar runding (*consultant*) perlu dilantik untuk proses menilai kebolehpayaan kontraktor dan sistem baru yang akan diperkenalkan atau dinaiktaraf.
- 11. Antara butir-butir yang perlu dinyatakan di dalam kontrak *outsourcing* adalah:
  - a. Kesahihan dan kerahsiaan logikal organisasi mesti dipelihara.
  - b. Pihak TUDM mesti membuat pengauditan terhadap sistem yang di *outsource*.

- c. Mesti menyatakan faktor keselamatan secara terperinci di dalam *Schedule Of Compliance (SOC)*.
  - d. Menyatakan pemilikan *source code* yang dibangunkan bersama dengan pihak *vendor* diserahkan kepada TUDM.
12. Pemindahan teknologi atau *Transfer Of Technology (TOT)* mesti dilaksanakan oleh kontraktor kepada pengguna.
13. Pihak kontraktor mesti menyediakan latihan yang dipersetujui untuk membolehkan TUDM mengurus dan menyenggara sistem ICT.
14. Projek *Outsourcing* pengauditan aset-aset ICT bertaraf rahsia ke atas tidak dibenarkan.
15. Capaian secara fizikal dan logikal mesti dipantau oleh wakil TUDM yang dilantik bagi menguruskannya.
16. *Intellectual Property Right (IPR)* untuk sistem yang dibangunkan atau pakej yang diubahsuai adalah menjadi hakmilik kerajaan mesti dinyatakan dalam perjanjian kontrak.

#### **PENGURUSAN TEKNIKAL KERENTANAN (VULNERABILITY)**

17. Memastikan pelaksanaan pengurusan teknikal kerentanan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya. Pengurusan teknikal kerentanan ini perlu dilaksanakan di atas sistem pengoperasian dan sistem aplikasi yang digunakan.
18. Perkara-perkara yang perlu dipatuhi adalah termasuk memperoleh maklumat teknikal kerentanan yang tepat pada masanya ke atas sistem maklumat yang digunakan, menilai tahap kerentanan tersebut dan mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.



**MANUAL PENGURUSAN KESELAMATAN ICT TUDM****BAHAGIAN 3****RISALAH 5****PENGURUSAN KESINAMBUNGAN PERKHIDMATAN****PENDAHULUAN**

1. Pengurusan Kesenambungan Perkhidmatan (*Business Continuity Management - BCM*) adalah mekanisma bagi mengurus dan memastikan kepentingan *stakeholder* sistem penyampaian perkhidmatan dilindungi dan imej TUDM terpelihara dengan mengenal pasti kesan dan impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan TUDM di samping menyediakan plan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan.
2. Pengurusan kesinambungan perkhidmatan dan plan pengurusan kesinambungan perkhidmatan diwujudkan dan dilaksanakan berdasarkan kepada persekitaran dan operasi TUDM.

**TUJUAN**

3. Menjamin operasi perkhidmatan agar tidak tergendala dan memastikan penyampaian perkhidmatan yang berterusan kepada pengguna.

**PLAN PENGURUSAN KESINAMBUNGAN PERKHIDMATAN**

4. Plan BCM hendaklah dibangunkan untuk memastikan pendekatan yang menyeluruh dilaksanakan bagi mengatasi gangguan ke atas aktiviti penyediaan perkhidmatan TUDM dan melindungi aktiviti daripada kesan bencana serta pemulihan perkhidmatan dalam tempoh yang ditetapkan. Perkara yang perlu dipatuhi adalah seperti berikut:
  - a. Mengenalpasti semua tanggungjawab dan prosedur kecemasan dan pemulihan.
  - b. Melaksanakan prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan.
  - c. Mendokumenkan proses dan prosedur yang telah dipersetujui.
  - d. Mengenalpasti peristiwa yang boleh mengakibatkan gangguan terhadap operasi TUDM serta impak ke atas keselamatan ICT.



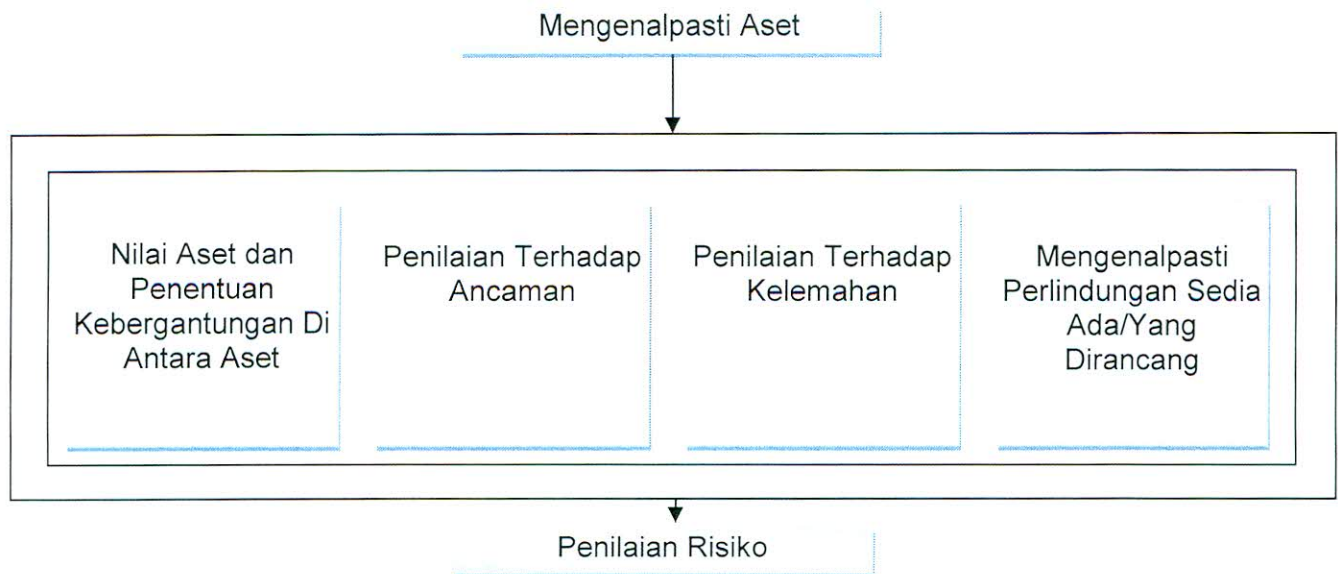
- e. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan.
  - f. Membuat *backup*.
  - g. Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.
5. Markas/Pangkalan/Unit adalah bertanggungjawab untuk memastikan operasi penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT TUDM.

#### **PENGURUSAN PENILAIAN RISIKO KESELAMATAN ICT**

6. Penilaian risiko keselamatan aset ICT bertujuan membolehkan TUDM mengukur, menganalisis tahap risiko aset ICT dan seterusnya mengambil tindakan untuk merancang dan mengawal risiko.

#### **TANGGUNGJAWAB MELAKSANAKAN PENILAIAN RISIKO KESELAMATAN ICT**

7. Markas/Pangkalan/Unit yang memiliki sistem ICT adalah bertanggungjawab kepada perkara-perkara berikut:
- a. Memastikan penilaian risiko keselamatan ICT dilaksanakan secara berkala dan berterusan. Keperluan melaksanakan penilaian risiko bergantung kepada perubahan persekitaran TUDM, teknologi semasa dan ancaman baru terhadap sistem ICT.
  - b. Mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.
  - c. Melaksanakan penilaian risiko mengikut peraturan atau prosedur yang ditetapkan oleh Kerajaan dari semasa ke semasa.
8. Proses analisis risiko keselamatan ICT perlu dilakukan oleh Bahagian Teknologi Maklumat dan Komunikasi (BTMK) sekurang-kurangnya sekali setahun. Proses pengurusan risiko adalah seperti di **Rajah 4**.



Rajah 4: Proses Pengurusan Risiko

9. Perkara-perkara yang perlu diambil kira sebelum analisa risiko ke atas ICT dilakukan adalah seperti berikut:

- a. Aset-aset ICT (perkakasan, perisian dan maklumat).
- b. Sumber Manusia (anggota TUDM, staf, kontraktor dan lain-lain individu luar).
- c. Persekitaran ICT (bangunan dan kemudahan).
- d. Aktiviti-aktiviti ICT (operasi, senggaraan dan pembangunan).

#### **SKOP PENILAIAN RISIKO KESELAMATAN ICT**

10. Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat TUDM termasuklah aplikasi, perisian, server, rangkaian dan/atau proses serta prosedur yang dikendalikan oleh TUDM. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuk Pusat Data, Bilik Media Storan, kemudahan utiliti dan sistem-sistem sokongan lain.

#### **PENENTUAN TINDAKAN UNTUK MENGENDALIKAN RISIKO KESELAMATAN ICT**

11. Setiap Markas/Pangkalan/Unit bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT masing-masing. Melalui proses-proses yang dilaksanakan untuk menilai risiko aset ICT Kerajaan, TUDM dapat mengenal pasti risiko-risiko yang wujud dan

seterusnya mengambil tindakan yang sewajarnya untuk menghadapi kemungkinan berlakunya risiko berkenaan.

12. Tindakan yang perlu diambil bagi menghadapi kemungkinan risiko terjadi adalah seperti berikut:

- a. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian.
- b. Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan TUDM.
- c. Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang sepatutnya.
- d. Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

13. Bahagian Teknologi Maklumat dan Komunikasi juga telah mewujudkan dokumen Pelan Kesenambungan Perkhidmatan bagi Pusat ICT TUDM sebagai panduan dalam menguruskan kesinambungan perkhidmatan bagi memastikan aset ict dilindungi dan mengurangkan sebarang risiko jika berlaku kecemasan. Sila rujuk **Pelan Kesenambungan Perkhidmatan TUDM ver 1.0** sebagai rujukan.



**MANUAL PENGURUSAN KESELAMATAN ICT TUDM****BAHAGIAN 3****RISALAH 6****PEMATUHAN****PENDAHULUAN**

1. Setiap pengguna ICT TUDM hendaklah membaca, memahami dan mematuhi Manual Keselamatan ICT, undang-undang atau peraturan-peraturan lain yang berkaitan dengannya. Pematuhan ini termasuk mendokumen dan mengemaskini keperluan-keperluan perundangan (*statutory*), peraturan dan ikatan kontrak.

**TUJUAN**

2. Meningkatkan tahap keselamatan ICT bagi mengelakkan pelanggaran Manual Keselamatan ICT TUDM, undang-undang jenayah dan sivil, peraturan atau ikatan kontrak dan sebarang keperluan keselamatan yang lain.

**PEMANTAUAN PEMATUHAN**

3. Semua aset ICT di TUDM termasuk maklumat yang disimpan di dalamnya adalah milik Kementerian Pertahanan, Ketua Jabatan/Bahagian, Perkhidmatan ATM amnya dan TUDM khususnya. Pemilik berhak memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.

**PEMATUHAN KEPERLUAN AUDIT**

4. Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.

**KEPERLUAN PERUNDANGAN**

5. Manual ini bertujuan memastikan rekabentuk, operasi, penggunaan dan pengurusan sistem maklumat adalah selaras serta berkeupayaan menghalang pelanggaran mana-mana keperluan perundangan, peraturan dan perjanjian yang berkuatkuasa. Perkara yang perlu dipatuhi adalah seperti berikut:

- a. Semua perlembagaan, undang-undang, peraturan, perjanjian yang dimeterai dan lain-lain perkara yang relevan kepada keselamatan sistem maklumat dan organisasi hendaklah dikenalpasti, didokumentasi dan dikemaskini.
  - b. Peraturan yang sesuai dilaksanakan untuk pematuhan ke atas perlembagaan, undang-undang dan keperluan kontrak mengenai penggunaan bahan yang tertakluk kepada hak milik harta intelek.
  - c. Rekod penting hendaklah dilindungi daripada hilang, rosak dan dipalsukan selaras dengan keperluan undang-undang, peraturan dan keperluan perjanjian TUDM.
  - d. Pengguna dilarang menggunakan kemudahan proses maklumat untuk tujuan yang tidak dibenarkan.
  - e. Penggunaan kriptografi dikawal selaras dengan perjanjian, perundangan dan peraturan yang berkuatkuasa.
6. Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di Markas/Pangkalan/Unit:
- a. Akta Rahsia Rasmi (Pindaan) 1986.
  - b. Semua Arahan Keselamatan berkaitan yang menyentuh perihal ICT.
  - c. Perintah-perintah semasa yang dikeluarkan oleh pihak Markas/Pangkalan/Unit.
  - d. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan".
  - e. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisma Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)".
  - f. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".



- g. Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk "Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam".
- h. Akta Tanda Tangan Digital 1997.
- i. Akta Jenayah Komputer 1997.
- j. Akta Hak Cipta (Pindaan) Tahun 1997.
- k. Akta Komunikasi dan Multimedia 1998.
- l. *Federal Armed Forces Security Instruction (FAFSI 1961)*.
- m. Akta Angkatan Tentera 1972.
- n. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS)*.
- o. Kripto Angkatan Tentera 1000 (KAT 1000).
- p. AIRSET 2001.
- q. PROTAP Sistem P4.
- r. Surat MAMPU dengan rujukan UPTM (S) 159/338/8 Jilid 30 (84) bertajuk "Langkah-langkah untuk memperkukuhkan keselamatan rangkaian setempat tanpa wayar (*Wireless Local Area Network*) di Agensi-agensi kerajaan.

#### **PELANGGARAN PERUNDANGAN**

7. Tindakan tatatertib boleh diambil ke atas sesiapa yang terlibat di dalam semua perbuatan kecuai, kelalaian dan pelanggaran keselamatan perkara-perkara berdarjah di bawah Akta Rahsia Rasmi (Pindaan) 1986 dan perintah-perintah semasa ATM dan TUDM.

#### **PEMATUHAN KEPADA DASAR, PIAWAIAN DAN TEKNIKAL KESELAMATAN**

8. Manual ini bertujuan memastikan keselamatan maklumat disemak sekurang-kurangnya setiap lima (5) tahun supaya mematuhi peraturan-peraturan di para 6. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:



- a. Pegawai penyelia hendaklah memastikan bahawa semua peraturan keselamatan dipatuhi selaras dengan perundangan, peraturan dan lain-lain keperluan keselamatan.
- b. Sistem maklumat hendaklah disemak dan diuji untuk memastikan pematuhan pelaksanaan piawaian keselamatan yang ditetapkan.
- c. ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawai dan keperluan teknikal.
- d. Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi piawai pelaksanaan keselamatan.
- e. Sebarang penilaian pematuhan teknikal seperti aktiviti *Security Posture Assessment* (SPA) mestilah dijalankan oleh individu yang kompeten dan dibenarkan.