Pejabat Timbalan Naib Canselor
(Pembangunan)

Universiti Teknologi MARA
40450 Shah Alam, Selangor, MALAYSIA
Tel : (+603) 5544 2299
Faks : (+603) 5521 1122
Emel : *tncpembangunan@uitm.edu.my*

UNIVERSITI TEKNOLOGI MARA

Surat Kami : 100-PPII(INFO.6/9)
Tarikh : 16 Mei 2019

SENARAI EDARAN

Tuan/Puan,

PEMAKLUMAN PROSES PERMOHONAN DOMAIN DAN FORENSIK DIGITAL

Dengan hormatnya perkara di atas adalah dirujuk.

2. Untuk makluman, pihak Bahagian Keselamatan ICT, Jabatan Infostruktur dalam usaha untuk mengurangkan risiko keselamatan laman web melalui pelaksanaan proses yang disediakan untuk kegunaan Pusat Tanggungjawab. Proses-proses tersebut adalah seperti berikut:-

i. Proses permohonan domain bagi sistem/web; dan
ii. Proses forensik digital apabila berlaku suatu insiden.

3. Mohon kerjasama daripada pihak tuan / puan untuk mengambil perhatian dan tindakan bagi proses-proses tersebut.

4. Segala kerjasama tuan/puan amatlah dihargai dan di dahului dengan ucapan terima kasih.

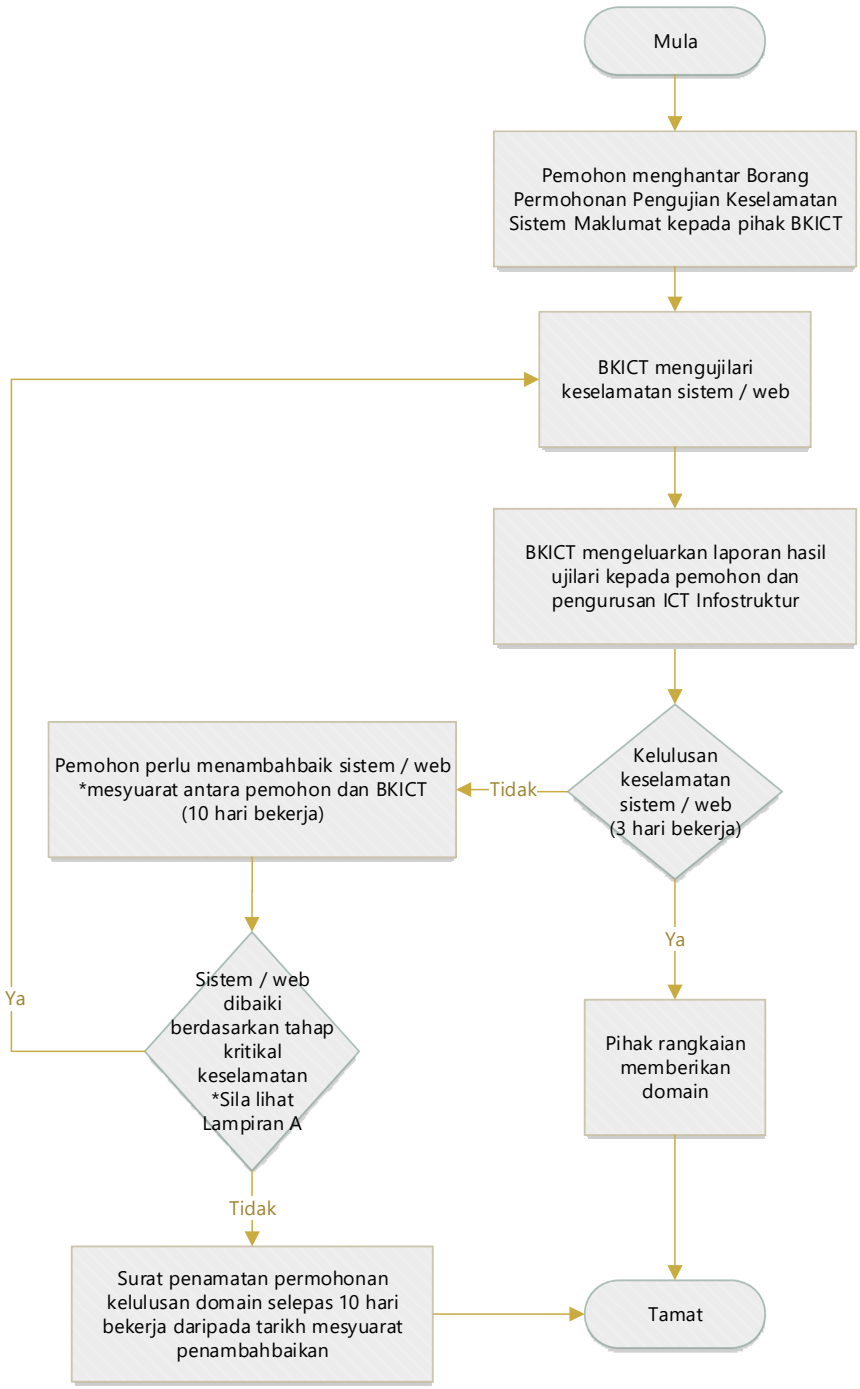
Sekian.

Yang benar

PROF. MAYDA DR MOHD FOZI ALI
Timbalan Naib Canselor (Pembangunan)

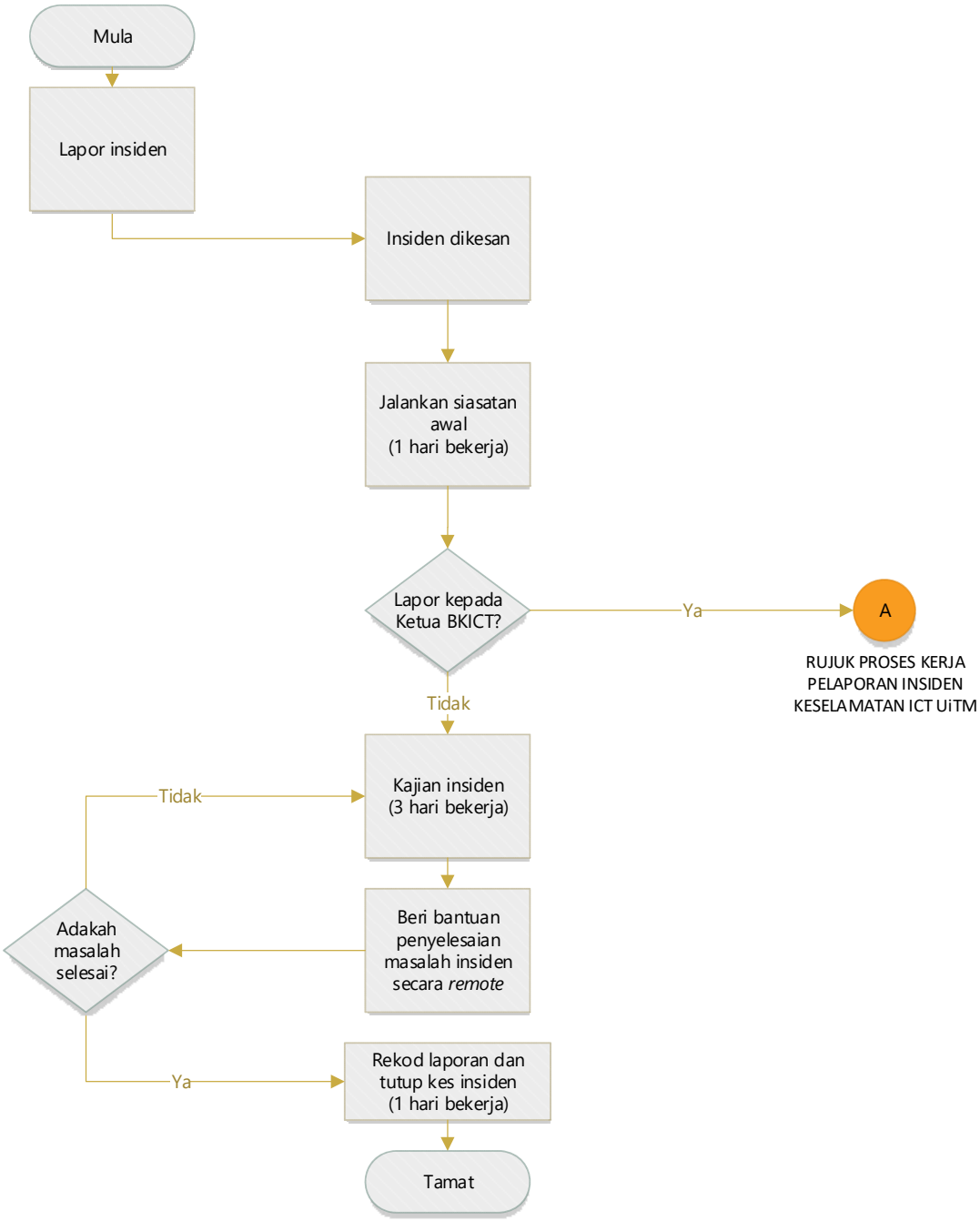
... disertakan

1. CARTA ALIR : PROSES KERJA PERMOHONAN DOMAIN BAGI SISTEM / WEB



BKICT = Bahagian Keselamatan ICT

2. CARTA ALIR : PROSES KERJA FORENSIK DIGITAL



BKICT = Bahagian Keselamatan ICT

LAMPIRAN A

1. Jenis insiden yang dikenalpasti adalah seperti berikut:

a) **Pelanggaran Dasar (*Violation of Policy*)**

Penggunaan aset ICT bagi tujuan kebocoran maklumat dan/atau mencapai maklumat yang melanggar Dasar Keselamatan ICT.

b) Penghalangan Penyampaian Perkhidmatan (*Denial of Service*)

Ancaman ke atas keselamatan sistem komputer di mana perkhidmatan pemprosesan maklumat sengaja dinafikan terhadap pengguna sistem. Ia melibatkan sebarang tindakan yang menghalang sistem daripada berfungsi secara normal. Termasuk *denial of service* (DoS), *distributed denial of service* (DDoS) dan *sabotage*.

c) **Pencerobohan (*Intrusion*)**

Mengguna dan mengubahsuai ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak. Ia termasuk capaian tanpa kebenaran, pencerobohan laman web, melakukan kerosakan kepada sistem (*system tampering*), pindaan data (*modification of data*) dan pindaan kepada konfigurasi sistem.

d) **Pemalsuan (*Forgery*)**

Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*) dan penipuan (*hoaxes*).

e) ***Spam***

Spam adalah emel yang dihantar ke akaun emel orang lain yang tidak dikenali penghantar dalam satu masa dan secara berulang-kali (kandungan emel yang sama). Ini menyebabkan kesesakan rangkaian dan tindak balas menjadi perlahan.

f) ***Malicious Code***

Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.

g) ***Harrassment/Threats***

Gangguan dan ancaman melalui pelbagai cara iaitu emel dan surat yang bermotif personal dan atas sebab tertentu.

h) ***Attempts/Hack Threats/Information Gathering***

Percubaaan (samada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran. Termasuk *spoofing, phishing, probing, war driving* dan *scanning.*

(i) **Kehilangan Fizikal (*Physical Loss*)**

Kehilangan capaian dan kegunaan disebabkan kerosakan, kecurian dan kebakaran ke atas aset ICT berpunca dari ancaman pencerobohan.

2. TAHAP KEUTAMAAN TINDAKAN KE ATAS INSIDEN

Tindakan ke atas insiden yang berlaku hendaklah dibuat berasaskan kepada keparahan sesuatu insiden. Tahap keutamaan tindakan ke atas insiden akan ditentukan seperti berikut :

a) Keutamaan 1 (Merah) – insiden keselamatan ICT yang membawa ancaman nyawa, menggugat keselamatan dan pertahanan negara, menjejas ekonomi dan imej negara, yang mungkin memerlukan Pelan Pemulihan Perkhidmatan (BCP) diaktifkan.

b) Keutamaan 2 (Kuning) – insiden keselamatan ICT selainnya seperti pencerobohan laman web, gangguan sistem dan pencerobohan aset ICT.