KERAJAAN MALAYSIA

SURAT PEKELILING AM BILANGAN 4 TAHUN 2022

GARIS PANDUAN SANITASI MEDIA ELEKTRONIK DALAM PERKHIDMATAN AWAM

JABATAN PERDANA MENTERI

9 Disember 2022

Dikelilingkan kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua YB Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri
Semua Pihak Berkuasa Tempatan

JABATAN PERDANA MENTERI
PRIME MINISTER'S DEPARTMENT
Blok B8, Kompleks Jabatan Perdana Menteri
Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya
MALAYSIA

Tel. : 03-8000 8000
Fax : 03-8888 3904
Web : http://www.jpm.gov.my
Emel : jpm@jpm.gov.my

Rujukan Kami: KPKK(R) 600-1/1 JLD.4 (15)

Tarikh: 9 Disember 2022

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua YB Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri
Semua Pihak Berkuasa Tempatan

SURAT PEKELILING AM BILANGAN 4 TAHUN 2022

GARIS PANDUAN SANITASI MEDIA ELEKTRONIK DALAM PERKHIDMATAN AWAM

1. TUJUAN

Garis panduan ini bertujuan sebagai sumber rujukan dan panduan kepada Jabatan bagi melaksanakan sanitasi media elektronik yang menyimpan maklumat rasmi dan rahsia rasmi Jabatan.

2. LATAR BELAKANG

Teknologi storan penyimpanan data semakin berkembang selari dengan penjanaan dan pendigitalan data yang meningkat mengikut arus pemodenan. Data dan maklumat Jabatan juga tidak terlepas daripada diproses dan disimpan melalui pelbagai medium dan media elektronik. Media tersebut ada di antaranya perlu melalui proses sanitasi bagi melupuskan maklumat apabila terdapat keperluan untuk berbuat demikian.

Oleh itu, Garis Panduan ini disediakan bagi membantu Jabatan di dalam melaksanakan sanitasi media elektronik mengikut amalan terbaik keselamatan berdasarkan kategori dan klasifikasi maklumat. Sanitasi media elektronik bertujuan untuk melupuskan data atau maklumat yang terkandung di dalamnya secara kekal dan merupakan langkah kawalan keselamatan bagi memastikan kerahsiaan maklumat rasmi dan rahsia rasmi Jabatan tidak terdedah kepada mana-mana pihak yang tidak dibenarkan. Proses pelupusan ini juga dibuat sebagai salah satu inisiatif keselamatan maklumat bagi menjamin integriti serta reputasi sesebuah Jabatan.

Garis Panduan ini juga dikeluarkan selaras dengan perenggan 143 dan 144, Arahan Keselamatan (Semakan dan Pindaan 2017).

3. PELAKSANAAN

Garis Panduan Sanitasi Media Elektronik Dalam Perkhidmatan Awam dilampirkan bersama surat pekeliling ini untuk rujukan dan pelaksanaan semua Jabatan.

4. PERANAN DAN TANGGUNGJAWAB KETUA JABATAN

Ketua Jabatan bertanggungjawab memastikan agar kerahsiaan data, maklumat dan rekod yang mungkin terdedah semasa proses sanitasi atau membaik pulih media elektronik dipelihara dan dijaga sepenuhnya. Ketua Jabatan hendaklah mengambil langkah-langkah sanitasi yang dibenarkan oleh pihak Kerajaan selari dengan kehendak undang-undang dan peraturan yang sedang berkuat kuasa.

5. KHIDMAT NASIHAT

Sebarang pertanyaan berkaitan dengan Surat Pekeliling ini boleh dikemukakan kepada:

Ketua Pegawai Keselamatan Kerajaan,
Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia,
Jabatan Perdana Menteri,
Aras -1,1 dan 2, Setia Perdana 7 ,
Kompleks Setia Perdana,
Pusat Pentadbiran Kerajaan Persekutuan,
62502 PUTRAJAYA.

Telefon : 03-8872 6038 / 6039
Faks : 03- 8888 3258
E-mel : kictrr@cgso.gov.my

6. PEMAKAIAN

Surat Pekeliling Am ini terpakai kepada semua agensi Perkhidmatan Awam Persekutuan bermula dari tarikh pekeliling ini ditandatangani. Tertakluk kepada penerimaannya oleh pihak berkuasa masing-masing, peruntukan Surat Pekeliling Am ini pada keseluruhannya dipanjangkan kepada semua Perkhidmatan Awam Negeri, Pihak Berkuasa Negeri dan Pihak Berkuasa Tempatan.

7. TARIKH KUAT KUASA

Surat Pekeliling ini berkuat kuasa mulai tarikh surat ini dikeluarkan.

Sekian, terima kasih.

"BERKHIDMAT UNTUK NEGARA"

(TAN SRI DATO' SERI MOHD ZUKI BIN ALI)
Ketua Setiausaha Negara

Lampiran kepada Surat Pekeliling Am Bilangan 4 Tahun 2022

KERAJAAN MALAYSIA

GARIS PANDUAN SANITASI MEDIA ELEKTRONIK DALAM PERKHIDMATAN AWAM

PEJABAT KETUA PEGAWAI KESELAMATAN KERAJAAN MALAYSIA

KANDUNGAN

AKRONIM

ATA	*Advanced Technology Attachment*
CIO	*Chief Information Officer* / Ketua Pegawai Maklumat
DOE	*Department of Environmental*
FPGA	*Field Programmable Gate Arrays*
GPS	*Global Positioning System*
HPA	*Host Protected Area*
ICTSO	*ICT Security Officer* / Pegawai Keselamatan ICT
OS	*Operating System*
PDA	*Personal Device Assistant*
PKJ	Pegawai Keselamatan Jabatan
RAM	*Random Access Memory*
ROM	*Read-Only Memory*
UMTS	*Universal Mobile Telecommunications System*
USB	*Universal Serial Bus*

TAFSIRAN

Dalam Garis Panduan ini, tafsiran yang digunakan adalah seperti berikut:

BIL.	TERMA	DEFINISI
1.	**Jabatan**	Sesebuah Kementerian, Jabatan Kerajaan, Badan Berkanun, Kerajaan Tempatan dan agensi lain yang kepadanya Akta 88 terpakai.
2.	**Jadual Pelupusan Rekod (JPR)**	Jadual yang mengenal pasti rekod yang mempunyai nilai arkib untuk dipelihara dan membenarkan pemusnahan rekod yang tinggal selepas luput tempoh pengekalan yang ditentukan – seksyen 27(3), Akta Arkib Negara 2003 [*Akta 629*].
3.	**Ketua Jabatan**	Termasuklah Ketua Setiausaha Kementerian, Setiausaha Kerajaan Negeri, Ketua Jabatan, Ketua sesuatu perkhidmatan, Ketua Badan Berkanun, Ketua Pejabat Kerajaan Tempatan, Ketua Cawangan Kecil sesebuah Jabatan dan Ketua bagi agensi lain yang kepadanya Akta 88 terpakai.
4.	**Media Elektronik**	Peralatan atau peranti yang digunakan untuk menyimpan maklumat rasmi dan rahsia rasmi termasuklah media storan seperti cakera keras (*hard disk*), cakera liut, cakera padat, pita magnetik, pita kaset, peranti mudah alih, *USB Flash Drive* dan seumpamanya.
5.	**Nilai Arkib**	Rekod yang dipelihara bagi nilai kebangsaan atau sejarahnya yang kekal dan lama bertahan atau kedua-duanya.
6.	**Pengelasan Semula**	Apa-apa rahsia rasmi boleh dilaksanakan pada bila-bila masa oleh Menteri atau pegawai awam yang dipertanggungkan dengan apa-apa tanggungjawab tentang mana-mana Kementerian, jabatan atau mana-mana perkhidmatan awam atau Menteri Besar atau

		Ketua Menteri sesuatu Negeri atau Ketua Pegawai yang menjaga hal ehwal pentadbiran sesuatu Negeri mengikut seksyen 2C Akta 88, atau mana-mana orang yang diturunkan kuasa oleh Menteri mengikut seksyen 5 Akta Perwakilan Kuasa 1956 [*Akta 358*]. Selepas pengelasan semula tersebut, rahsia rasmi itu hendaklah terhenti menjadi rahsia rasmi.
7.	**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 memberikan keuntungan besar kepada sesebuah kuasa asing hendaklah diperingkatkan sebagai "Rahsia".
8.	**Rahsia Besar**	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia, hendaklah diperingkatkan sebagai "Rahsia Besar".
9.	**Rahsia Rasmi**	Apa-apa suratan yang dinyatakan dalam Jadual kepada Akta 88 dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai "Rahsia Besar", "Rahsia", "Sulit" atau "Terhad" mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu Negeri atau mana-mana pegawai awam yang dilantik bawah seksyen 2B Akta 88.
10.	**Rasmi**	Adalah berhubungan dengan perkhidmatan awam.
11.	**Rekod Elektronik**	Merupakan maklumat yang diwujudkan, diterima dan disimpan secara digital.

GARIS PANDUAN SANITASI MEDIA ELEKTRONIK DALAM PERKHIDMATAN AWAM

1. PENGENALAN

1.1 TUJUAN

Garis Panduan ini bertujuan sebagai sumber rujukan dan panduan kepada Jabatan yang beroperasi di dalam dan luar negara bagi melaksanakan sanitasi media elektronik yang menyimpan maklumat rasmi dan rahsia rasmi Jabatan.

Dokumen ini membantu Jabatan di dalam melaksanakan sanitasi dengan mengambil langkah-langkah yang dibenarkan oleh pihak Kerajaan selari dengan kehendak undang-undang dan peraturan yang sedang berkuat kuasa.

1.2 KEPERLUAN UNTUK MEWUJUDKAN KAEDAH SANITASI YANG BETUL

Sanitasi merujuk kepada proses untuk menjadikan capaian akses ke atas data atau maklumat yang terkandung dalam media elektronik tidak lagi dapat dilaksanakan walaupun dengan tahap usaha yang tertentu**.** Sanitasi media elektronik merupakan satu elemen penting semasa proses pelupusan data/maklumat bagi memelihara kerahsiaan maklumat. Ini termasuklah kawalan terhadap maklumat yang mengandungi rahsia rasmi dan media elektronik yang berfungsi sebagai medium penyimpanan maklumat tersebut. Proses sanitasi boleh menghapuskan data serta maklumat secara kekal dan tidak boleh diguna pakai atau dimanipulasi oleh mana-mana pihak yang mempunyai kepentingan tertentu. Proses sanitasi ini juga dibuat sebagai salah satu inisiatif keselamatan maklumat bagi menjamin integriti serta reputasi sesebuah organisasi.

Ketua Jabatan perlu memastikan agar kerahsiaan data, maklumat dan rekod yang mungkin terdedah semasa sanitasi atau pun membaik pulih media elektronik dipelihara dan dijaga sepenuhnya. Risiko pencerobohan ke atas media elektronik boleh dikurangkan melalui pemahaman mengenai:

i. Tahap klasifikasi atau pengelasan data, maklumat dan rekod kerajaan; dan

ii. Kaedah perlindungan data, maklumat dan rekod kerajaan.

1.3 SKOP

Garis panduan ini terpakai bagi semua media elektronik yang mengandung data, maklumat dan rekod rasmi serta rahsia rasmi Jabatan di dalam persekitaran teknologi maklumat dan komunikasi (ICT).

1.4 DOKUMEN-DOKUMEN YANG BERKAITAN

Garis panduan ini hendaklah dibaca bersekali dengan peraturan yang sedang berkuat kuasa seperti berikut:

a. Akta Rahsia Rasmi 1972 [*Akta 88*];
b. Akta Tandatangan Digital 1997 [*Akta 562*];
c. Akta Komunikasi dan Multimedia 1998 [*Akta 588*];
d. Akta Aktiviti Kerajaan Elektronik 2007 [*Akta 680*];
e. Arahan Keselamatan (Semakan dan Pindaan 2017);
f. Arahan Teknologi Maklumat 2007;
g. Bab IV Pengurusan Rekod, Akta Arkib Negara 2003 [*Akta 629*];
h. Surat Pekeliling Perbendaharaan Bil. 1 Tahun 1991 (Garis Panduan Pelupusan Peralatan Komputer);
i. Surat Pekeliling Perbendaharaan Bil. 5/2007 (Tatacara Pengurusan Aset Alih Kerajaan);
j. *Guidelines for Classification of Used Electrical and Electronic Equipment in Malaysia - Department of Environmental (DOE)*;
k. Surat Pekeliling Am Bilangan 2 Tahun 2021 (Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (*Cloud Computing*) Dalam Perkhidmatan Awam);
l. Jadual Pelupusan Rekod. Rujuk panduan-panduan Arkib Negara Malaysia; dan
m. Arahan-arahan lain yang sedang berkuat kuasa.

2. MEDIA STORAN, DATA, MAKLUMAT DAN REKOD ELEKTRONIK KERAJAAN

Perkembangan teknologi maklumat dan komunikasi (ICT) pada masa kini telah banyak merubah cara kehidupan dan cara kerja di kalangan pegawai awam. Penggunaan teknologi yang pesat dalam semua aspek pentadbiran kerajaan telah membawa kepada penjanaan rekod elektronik yang semakin bertambah. Penjanaan rekod elektronik ini memerlukan media storan yang sesuai untuk menyimpan kesemua rekod tersebut.

Di antara media-media storan dan kaedah yang digunakan untuk menyimpan data, maklumat dan rekod elektronik seperti berikut:

i. Tidak Kekal (*volatile*) - Apabila kuasa elektrik dimatikan, rekod yang disimpan dalam memori utama tidak dapat dicapai, walaupun masih wujud dalam ruang memori berkenaan. Contoh penyimpanan tidak kekal ialah ingatan capaian rawak (*Random Access Memory*, RAM);

ii. Kekal (*non-volatile*) - Apabila kuasa elektrik dimatikan, rekod tersebut masih lagi wujud dalam ruang storan berkenaan dan dapat dicapai. Contoh storan kekal adalah seperti *hard disk*, USB, *optical disk*, cakera liut (*floppy disk*), ROM; dan

iii. Sebarang peralatan elektronik yang berupaya menyimpan data dan maklumat atau setara dengannya.

2.1 KAEDAH SANITASI

Terdapat beberapa kaedah sanitasi yang boleh dilaksanakan berdasarkan kepada jenis media elektronik yang digunakan. Sanitasi ini dibahagikan kepada dua (2) kategori utama iaitu:

2.1.1 Sanitasi Logikal

Sanitasi logikal ialah proses menulis ganti (*overwriting*) data yang berada dalam media elektronik secara logikal. Proses ini boleh dilakukan dengan menggunakan perisian yang berupaya melakukan sekurang-kurangnya tiga (3) kali *overwrite* bagi memastikan data benar-benar dipadamkan. Kaedah ini lebih menjimatkan berbanding sanitasi fizikal, tetapi sanitasi logikal hanya mampu menghapuskan data yang dikehendaki. Walau bagaimanapun kaedah ini tidak mampu menghapuskan keseluruhan kandungan media elektronik seperti contoh *Host Protected Area* (HPA).

Sanitasi logikal terbahagi kepada empat (4) kategori iaitu:

i. **Sanitasi Fail** (hanya boleh dilaksanakan sekiranya fail tersebut boleh dilihat oleh Sistem Pengoperasian (OS));

ii. **Sanitasi *Partition*** (kaedah ini dilaksanakan sekiranya hanya sebahagian daripada ruang storan hendak dilupuskan);

iii. **Sanitasi Media Storan** (kaedah ini dilakukan sekiranya keseluruhan ruang media storan hendak dilupuskan); dan

iv. **Tetapan asal** (*Factory Setting*) (sila rujuk kepada manual yang dikeluarkan oleh pengeluar untuk set semula media elektronik kepada tetapan asal).

Adalah diingatkan sesetengah media elektronik tidak boleh disanitasi dengan cara *overwrite* dan perlu disanitasi dengan cara lain.

2.1.2 Sanitasi Fizikal

Sanitasi fizikal adalah menulis ganti data yang berada dalam media elektronik secara fizikal. Terdapat tiga (3) kaedah untuk melakukan sanitasi fizikal iaitu:

a. Tulis ganti (*Overwrite*)

Proses tulis ganti secara fizikal ialah menulis ganti keseluruhan data yang terdapat dalam media elektronik secara fizikal. Proses ini dilakukan dengan menggunakan perkakasan yang sesuai. Proses ini haruslah dilakukan sekurang-kurangnya tiga (3) kali bagi memastikan data benar-benar terhapus. Tulis ganti secara fizikal akan menghasilkan keputusan yang sama seperti sanitasi logikal, tetapi proses tulis ganti secara fizikal dilakukan dengan lebih cepat. Tulis ganti secara fizikal mampu menghapuskan keseluruhan data dalam sesuatu media elektronik. Proses ini bagaimanapun, tidak mampu menghapuskan *default data*, seperti contoh HPA. HPA kebiasaannya tidak mengandungi data pengguna sebaliknya mengandungi data asal (*manufacturer data*).

b. Penyingkiran (*Purging*)

Penyingkiran merupakan satu kaedah yang dapat memastikan data tidak boleh dibina semula (*reconstructed*) dengan mana-mana teknik yang diketahui. Penyingkiran ialah satu lagi kaedah yang menjamin kemusnahan data secara keseluruhan. Terdapat dua (2) jenis kaedah penyingkiran iaitu:

i. melaksanakan arahan *Secure Erase* terhadap *firmware* media storan tersebut. Walau bagaimanapun cara ini hanya boleh digunakan terhadap media storan *Advanced Technology Attachment* (ATA) sahaja; dan

ii. melaksanakan *degaussing* iaitu proses memadam keseluruhan data yang terkandung dalam media storan dengan mendedahkannya kepada medan magnetik yang kuat. Kaedah ini akan menyebabkan data di dalam media, *hard disk platter* dan *firmwar*e akan dipadamkan. *Degaussing* akan menyebabkan media tersebut tidak boleh diguna pakai lagi. Kaedah ini hanya boleh digunakan untuk media storan yang menggunakan medan magnetik untuk menyimpan data, iaitu *hard disk*. Teknik ini tidak sesuai bagi *flash memory* seperti *pen drive* da*n memory card* kerana ia memanipulasikan medan elektronik untuk menyimpan data.

c. Pemusnahan (*Destroying*)

i. Pemusnahan merupakan satu kaedah pada kebiasaannya akan digunakan sekiranya media storan tidak lagi dapat digunakan dan teknik *purging* gagal dilaksanakan ke atas media tersebut. Kaedah pemusnahan biasanya melibatkan kategori media elektronik yang mempunyai peringkat keselamatan yang tinggi (rahsia dan rahsia besar). Selepas pemusnahan, sebarang proses pemulihan data ke atas media tersebut tidak lagi boleh dilakukan sekalipun melalui teknik makmal (*laboratory technique*);

ii. Penandaan luar (secara fizikal) yang menunjukkan kegunaan, label inventori atau tanda pengelasan pada media elektronik hendaklah dipadamkan atau ditanggalkan kesemuanya sebelum kaedah ini dilaksanakan; dan

iii. Terdapat pelbagai jenis, teknik dan prosedur bagi pemusnahan media elektronik seperti penghancuran/ penyepaian (*disintegration*), kisaran halus (*pulverization*), peleburan dan pembakaran. Kaedah-kaedah sanitasi ini direka bentuk bagi memusnahkan media elektronik. Secara

lazimnya juga, penglibatan pihak ketiga yang mempunyai keupayaan khusus seperti kemudahan pembakaran berlesen, pemusnahan peralatan elektronik (logam) adalah perlu dirujuk bagi melancarkan proses pemusnahan agar ia lebih efektif dan selamat.

2.1.3 Kaedah-kaedah Lain Sanitasi

Terdapat beberapa kaedah sanitasi yang mungkin tidak dinyatakan di dalam dokumen ini tetapi kaedah berkenaan masih boleh dipertimbangkan dan sesuai untuk digunakan. Perubahan teknologi pada media elektronik boleh menghasilkan pelbagai kaedah sanitasi dan ia boleh diterima pakai sekiranya kaedah tersebut berupaya untuk memenuhi objektif keselamatan dan berdasarkan amalan terbaik keselamatan. Rujukan ke Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia hendaklah dibuat sekiranya Jabatan mempunyai kaedah-kaedah lain selain yang dinyatakan di dalam dokumen ini.

2.2 FAKTOR YANG PERLU DIPERTIMBANGKAN DALAM MEMILIH KAEDAH SANITASI

Dalam membuat keputusan mengenai kaedah sanitasi yang ingin dilaksanakan, beberapa faktor perlu dipertimbangkan oleh Jabatan. Di antara faktor-faktor yang perlu dipertimbangkan oleh Jabatan meliputi perkara-perkara berikut:

a. mengkaji secara terperinci jenis media elektronik yang hendak disanitasi, termasuklah menilai keupayaan, keberkesanan dan prestasi media elektronik tersebut;

b. kenal pasti peringkat keselamatan maklumat yang disimpan dan jenis media elektronik yang digunakan. Rahsia rasmi termasuk data, maklumat dan rekod elektronik yang terkandung dalam media elektronik tersebut masih mempunyai implikasi

keselamatan dan nilai arkib (seperti mana yang ditetapkan di dalam Jadual Pelupusan Rekod yang telah disediakan oleh Jabatan bersama dengan Arkib Negara Malaysia) hendaklah dibuat salinan bagi tujuan pemeliharaan dan kawalan keselamatan. Walau bagaimanapun kelulusan pemusnahan hendaklah diperoleh terlebih dahulu daripada Ketua Pengarah Arkib Negara Malaysia/Arkib Negeri Sabah/Pustaka Sarawak, Akauntan Negara/Negeri, Audit Negara/Negeri/Bendahari Negeri;

c. menentukan proses sanitasi dilaksanakan sama ada di peringkat Jabatan atau oleh pihak ketiga berdasarkan kepada keupayaan sesebuah Jabatan. Sekiranya Jabatan melaksanakan sanitasi media elektronik, proses dan peralatan yang digunakan hendaklah mengikut peraturan yang telah ditetapkan dalam garis panduan ini, Jabatan Alam Sekitar atau mana-mana Jabatan yang berkaitan;

d. menilai dan memastikan individu yang melaksanakan proses sanitasi media elektronik mempunyai kompetensi dan kemahiran mengendalikannya. Individu berkenaan hendaklah tidak terlibat secara langsung ke atas pengurusan media elektronik yang hendak dilupuskan;

e. tempoh masa penyimpanan data, maklumat dan rekod rahsia rasmi adalah tertakluk pada tempoh simpanan yang dinyatakan dalam Jadual Pelupusan Rekod untuk mengelakkan proses sanitasi yang boleh menjejaskan perkhidmatan Jabatan berkenaan; dan

f. memastikan kaedah sanitasi yang dipilih adalah bersesuaian dengan nilai maklumat dan media elektronik bagi memelihara rahsia rasmi daripada pendedahan yang tidak dibenarkan. Contoh pelaksanaan sanitasi media elektronik berdasarkan

kepada peringkat keselamatan maklumat dan kaedah sanitasi adalah seperti di Lampiran A.

3. PERANAN DAN TANGGUNGJAWAB

3.1 KETUA JABATAN

Ketua Jabatan bertanggungjawab menentukan tadbir urus sanitasi media elektronik yang menyimpan maklumat rasmi dan rahsia rasmi dilaksanakan dengan mengguna pakai Jawatankuasa Menyemak, Menilai dan Mengelaskan Semula Rahsia Rasmi yang sedia ada bagi tujuan sanitasi media elektronik. Ketua Jabatan juga hendaklah memastikan latihan berkaitan sanitasi diberikan secukupnya kepada kakitangan Jabatan dan memastikan supaya semua kakitangan di bawah seliaannya atau pengguna mematuhi kepada garis panduan ini.

3.2 PEGAWAI KESELAMATAN JABATAN / KETUA PEGAWAI MAKLUMAT

Pegawai Keselamatan Jabatan (PKJ) / Ketua Pegawai Maklumat (CIO) bertanggungjawab dalam pematuhan dasar, amalan terbaik global dan piawaian ICT untuk memastikan kejayaan pelaksanaan sistem aplikasi ICT. Struktur tadbir urus pengurusan sanitasi media elektronik yang menyimpan maklumat rasmi dan rahsia rasmi hendaklah dinyatakan di dalam polisi keselamatan ICT Jabatan seperti DKICT, ISMS dan lain-lain. Prosedur yang berkaitan dengan sanitasi media elektronik perlu dibangunkan, didokumenkan, diterbitkan, dibudayakan dan dikemas kini selaras dengan perkembangan teknologi, amalan terbaik serta mengikut garis panduan asas yang telah ditetapkan oleh pihak Kerajaan.

3.3 PEGAWAI KESELAMATAN ICT

Pegawai Keselamatan ICT (ICTSO) berperanan dalam menguatkuasakan polisi dan prosedur yang telah dibangunkan. Dasar berkaitan proses sanitasi media elektronik dan kawalan keselamatan maklumat hendaklah dilaksanakan

dan sentiasa dipraktikkan mengikut kaedah yang bersesuaian di seluruh Jabatan. Analisis risiko merupakan faktor penting yang perlu dilaksanakan oleh ICTSO sebelum pelaksanaannya.

3.4 PEGAWAI ASET

Pegawai Aset bertanggungjawab untuk memastikan media elektronik perlu menjalani proses sanitasi sebelum dimusnahkan atau didermakan mengikut prosedur dan peraturan yang telah ditetapkan.

3.5 PENGURUS REKOD

Pengurus Rekod bertanggungjawab dalam menyampaikan khidmat nasihat kepada pemilik sistem/data bahawa **rekod yang mempunyai kepentingan kebangsaan, sejarah dan penyelidikan hendaklah dikenal pasti dan dipelihara** agar sanitasi media elektronik tidak memusnahkan sebarang **rekod elektronik** yang masih perlu dilindungi. Pengurus rekod hendaklah bekerjasama dengan Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia dan Arkib Negara Malaysia bagi mematuhi keperluan perundangan, peraturan serta piawaian sedia ada.

3.6 PENGGUNA

Pengguna bertanggungjawab untuk mengetahui, memahami dan memastikan maklumat rahsia rasmi di bawah kawalan mereka dilindungi dan mematuhi sanitasi rahsia rasmi berdasarkan keperluan garis panduan yang telah ditetapkan.

4. KEPUTUSAN MELAKSANA SANITASI

4.1 MENGENALPASTI KEPERLUAN SANITASI

Langkah awalan di dalam membuat keputusan adalah mengkaji sekiranya terdapat keperluan untuk menjalankan proses sanitasi media elektronik. Jabatan perlu mengenal pasti media elektronik yang berkeupayaan untuk menyimpan data dan perlu memahami keadaan mana yang boleh menyebabkan media tersebut perlu disanitasi.

4.2 MENENTUKAN PERINGKAT KESELAMATAN

Pengelasan data, maklumat dan rekod rahsia rasmi hendaklah berpandukan kepada peraturan dan arahan yang berkuat kuasa. Kategori pemeringkatan ini akan memudahkan Jabatan menentukan proses sanitasi mengikut kepada peringkat keselamatan media elektronik. Media elektronik ini hendaklah dilabel selaras dengan peruntukan Arahan Keselamatan (Semakan dan Pindaan 2017). Kandungan maklumat/rekod yang terkandung di dalam media elektronik hendaklah dinilai bagi menentukan sama ada ia adalah maklumat rasmi atau rahsia rasmi.

4.3 PENGELASAN SEMULA

Jabatan hendaklah memastikan media elektronik yang hendak disanitasi merupakan inventori dan aset Jabatan di bawah hak miliknya sendiri. Media elektronik yang bukan hak milik Jabatan (sewaan) dan mengandung maklumat rahsia rasmi jika terdapat keperluan hendaklah dikelaskan semula terlebih dahulu sebagaimana diperuntukkan di bawah seksyen 2C Akta Rahsia Rasmi 1972 [*Akta 88*]. Pengelasan semula media elektronik hanya perlu dilaksanakan sekiranya maklumat rahsia rasmi yang diwujudkan dalam sistem ICT dan tidak dijana secara fizikal.

Maklumat rahsia rasmi yang telah dikelaskan semula hendaklah didaftarkan di dalam Buku Daftar Am Suratan Rahsia Rasmi (Am 492 & 492B), diselenggarakan dari semasa ke semasa dan mesti ditandatangani oleh pegawai yang diberi kuasa di bawah seksyen 2C Akta 88.

4.4 PENGGUNAAN SEMULA MEDIA ELEKTRONIK

Perancangan penggunaan semula sesuatu media elektronik atau tidak akan menentukan pemilihan kaedah sanitasi. Kaedah sanitasi fizikal disyorkan sekiranya media elektronik tersebut tidak akan diguna semula.

4.5 KAWALAN AKSES SEMASA SANITASI DAN PENYELENGGARAAN

Media elektronik yang digunakan oleh Jabatan memerlukan penyelenggaraan dari semasa ke semasa. Kawalan akses ke atas media elektronik yang diselenggarakan oleh pihak pembekal atau pihak ketiga perlu dilaksanakan untuk menjamin kerahsiaan data, maklumat dan rekod rahsia rasmi terpelihara. Oleh itu, perkara-perkara berikut perlu dipatuhi:

a. kerja-kerja sanitasi media elektronik yang dijalankan secara *on-site* hendaklah diselia oleh Jabatan;

b. sekiranya media elektronik ini akan dipulangkan kepada pihak pembekal disebabkan kerosakan kekal dan/atau perlu ditukar ganti, persetujuan di antara pihak Jabatan dan pihak pembekal hendaklah dicapai bagi memastikan media elektronik disanitasi dengan selamat; dan

c. pihak Jabatan bertanggungjawab untuk memastikan kontrak penyelenggaraan yang dimeterai dengan pihak pembekal atau pihak ketiga mengambil kira proses sanitasi media elektronik.

4.6 KEPUTUSAN UNTUK SANITASI

Proses akhir membuat keputusan adalah bersandarkan kepada pengelasan data, maklumat, rekod rasmi dan rahsia rasmi serta tahap risiko dan bukannya jenis media elektronik.

Namun begitu, pelaksanaan sanitasi juga bergantung pada:

a. faktor demografi;

b. tempoh masa memperoleh kelulusan daripada pihak-pihak yang berkaitan sebelum pelaksanaan sanitasi seperti Arkib Negara Malaysia/Arkib Negeri Sabah/Pustaka Sarawak, Akauntan Negara/Negeri, Audit Negara/Negeri, Bendahari Negeri dan lain-lain pihak berkuasa yang berkaitan; dan

c. kawalan keselamatan fizikal dan persekitaran ICT sesebuah Jabatan.

Setelah keputusan akhir dibuat, keputusan sanitasi perlu didokumenkan dan memastikan bahawa proses dan sumber-sumber yang tepat adalah dirujuk bagi menyokong keputusan ini.

4.7 PENGESAHAN SANITASI (VALIDASI)

Pengesahan sanitasi media elektronik hendaklah dilaksanakan bagi memastikan data, maklumat, rekod rasmi dan rahsia rasmi telah dilupuskan dan tidak boleh diperoleh semula dengan apa jua cara. Sampel media elektronik yang telah menjalani sanitasi hendaklah diuji secara telus. Proses pengesahan ini hendaklah dilaksanakan oleh pihak yang tidak mempunyai sebarang kepentingan atau penglibatan khusus di dalam sanitasi media elektronik ini dan kompeten bagi menjalankan setiap tugas tersebut.

4.8 DOKUMENTASI

Setiap aktiviti sanitasi media elektronik hendaklah direkodkan dengan jelas bagi menjamin akauntabiliti pengurusan sanitasi tersebut. Rekod sanitasi media elektronik hendaklah meliputi proses pengelasan semula, pemeliharaan rekod dan pengesahan sanitasi oleh pihak berwajib.

4.9 KAWALAN PERSEKITARAN

Sanitasi media elektronik secara fizikal perlu mematuhi keperluan undang-undang yang telah ditetapkan oleh Jabatan Alam Sekitar. Proses sanitasi media elektronik melibatkan peralatan elektrik dan elektronik yang terdiri dari komponen-komponen tertentu boleh menjejaskan alam sekitar sekiranya pertimbangan awal tidak dilakukan sewajarnya.

5. TADBIR URUS SANITASI MEDIA ELEKTRONIK

5.1 JAWATANKUASA PELAKSANAAN

Jabatan boleh mengguna pakai Jawatankuasa Menyemak, Menilai dan Mengelaskan Semula Rahsia Rasmi yang sedia ada bagi tujuan pelupusan dengan penambahan ahli jawatankuasa yang bersesuaian sepertimana berikut:

a. Pegawai Keselamatan Jabatan (PKJ) / Ketua Pegawai Maklumat (CIO);
b. Pegawai Keselamatan Kerajaan (selaku penasihat);
c. Pegawai Arkib Negara;
d. Pegawai Jabatan Alam Sekitar;
e. Pegawai Keselamatan ICT (ICTSO);
f. Pegawai Aset;
g. Pengurus Rekod; dan
h. Pengguna.

5.2 PERANAN JAWATANKUASA

Peranan Jawatankuasa adalah seperti berikut:

a. bertanggungjawab dalam menilai, menyemak dan membuat keputusan bagi melaksanakan sanitasi media elektronik (sila rujuk Lampiran C);

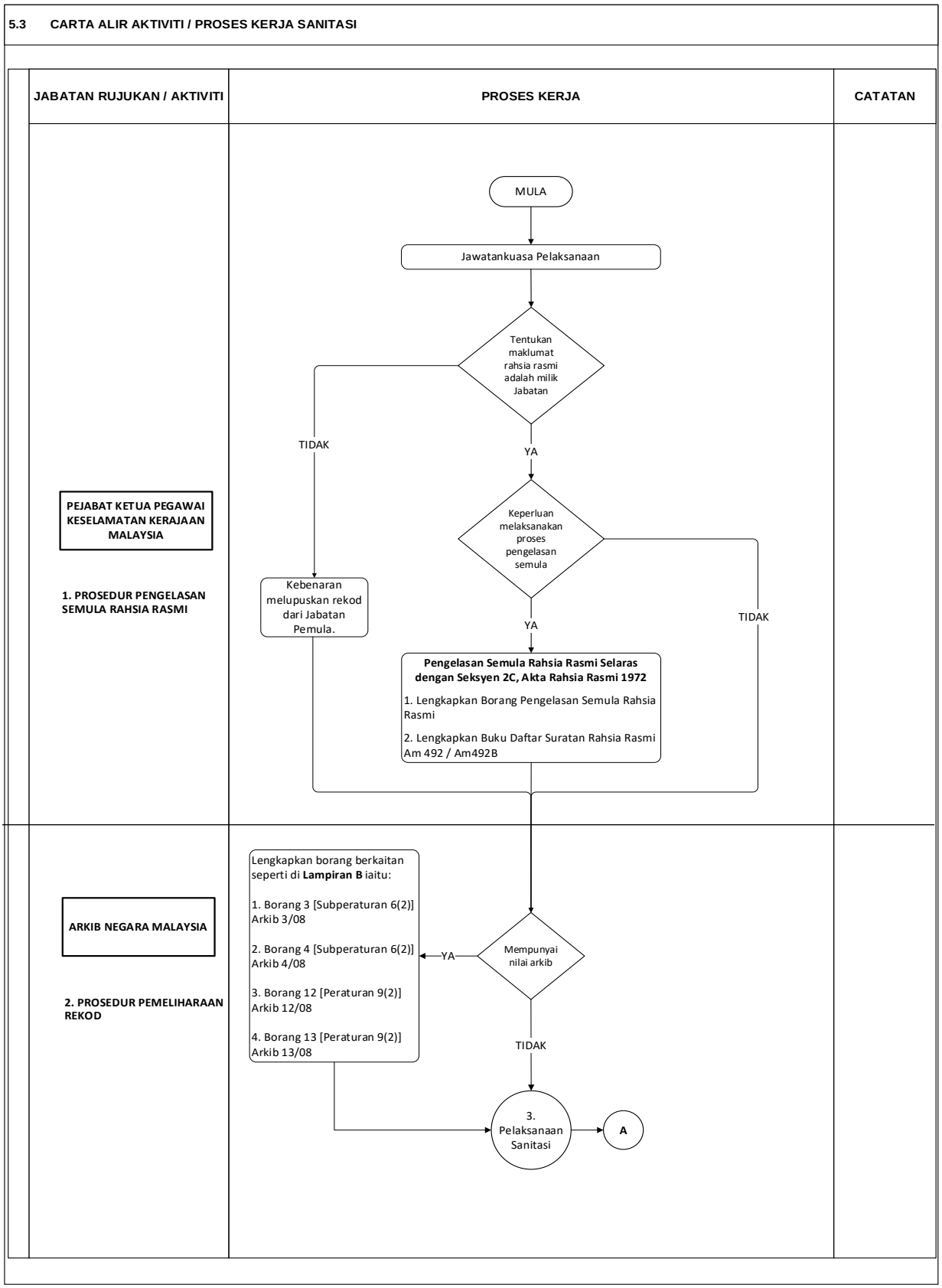
b. mengemukakan satu laporan penilaian risiko berserta syor cadangan sanitasi kepada Ketua Jabatan;

c. menyemak dan memastikan proses sanitasi media elektronik memenuhi aspek perundangan dan pentadbiran yang berkuat kuasa; dan

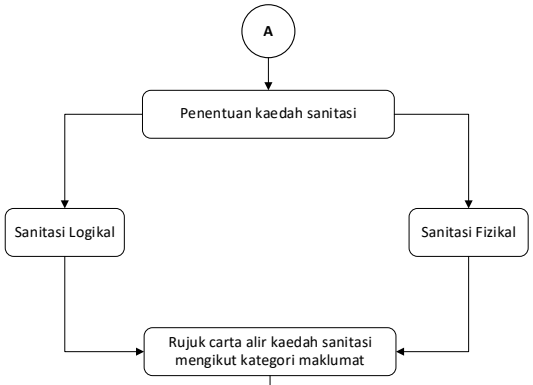
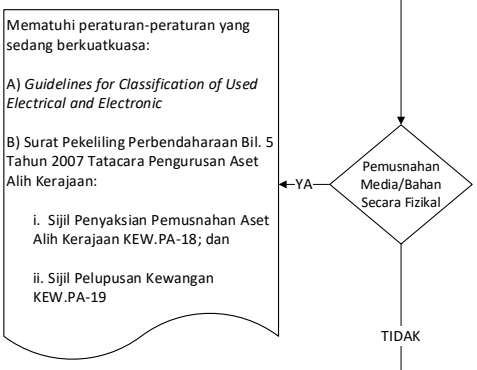
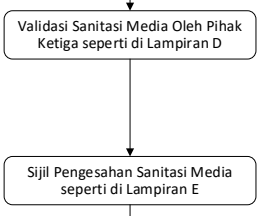
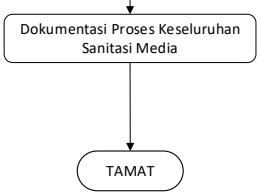
d. memperakukan sanitasi media elektronik dan segala urusan didokumenkan dan difailkan.

5.3 CARTA ALIR AKTIVITI / PROSES KERJA SANITASI

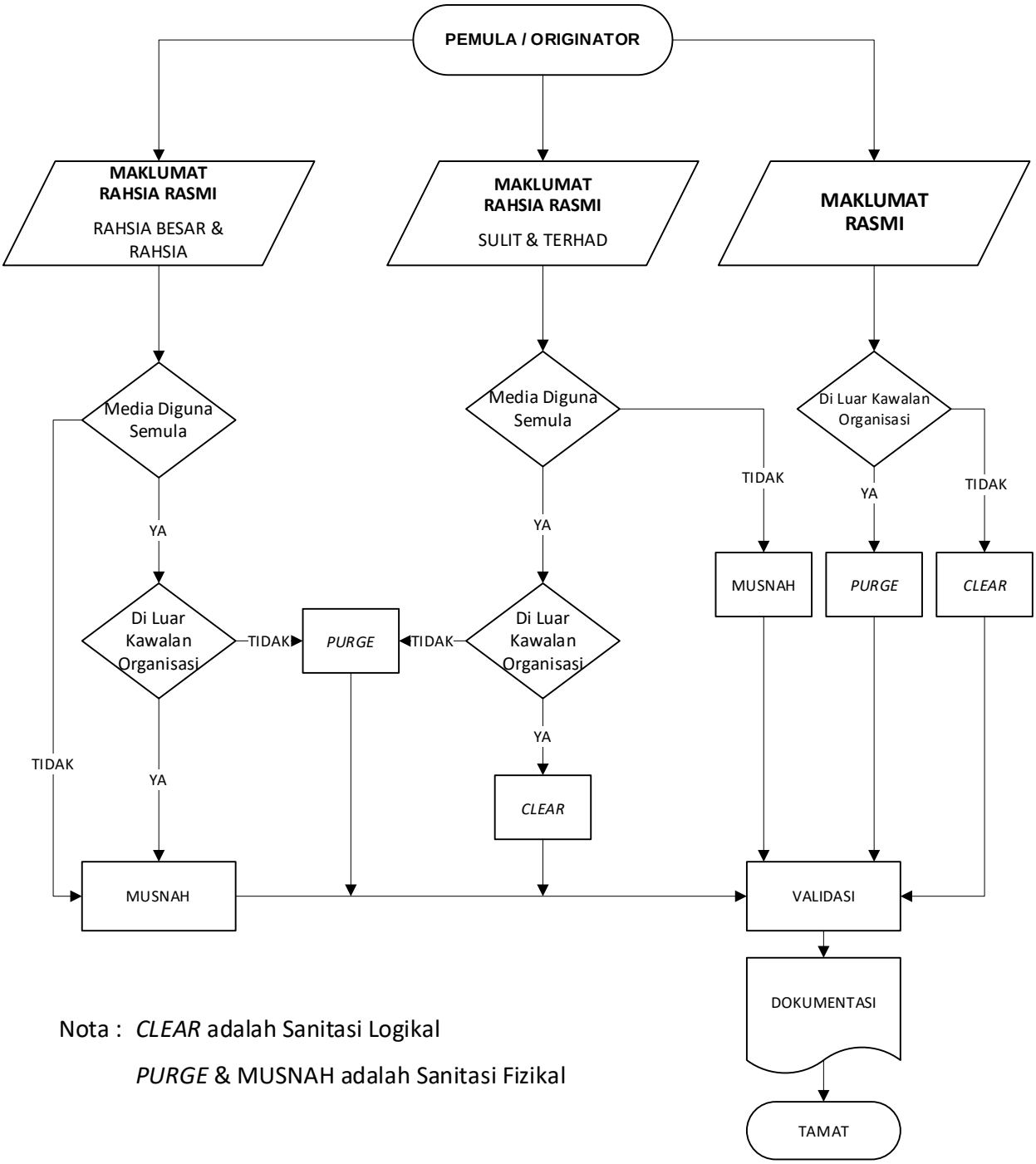
Carta alir aktiviti dan proses kerja sanitasi adalah seperti berikut:



5.3 CARTA ALIR AKTIVITI / PROSES KERJA SANITASI

JABATAN RUJUKAN / AKTIVITI	PROSES KERJA	CATATAN
JABATAN / AGENSI **3.PELAKSANAAN SANITASI**		
JABATAN ALAM SEKITAR / JABATAN / AGENSI **4. PROSEDUR PEMUSNAHAN BAHAN**		
5. VALIDASI		
6. DOKUMENTASI		Nombor Rujukan Fail

5.4 CARTA ALIR KAEDAH SANITASI MENGIKUT KATEGORI MAKLUMAT



Nota : *CLEAR* adalah Sanitasi Logikal

PURGE & MUSNAH adalah Sanitasi Fizikal

6. PENUTUP

Terdapat beberapa media elektronik mudah dilupuskan dan tidak memberi kesan terhadap pengurusan Jabatan, tidak menghasilkan kerugian atau kehilangan aset mahupun mendatangkan kecederaan kepada individu. Bagi media elektronik yang terdiri daripada alat-alat atau bahan-bahan yang digunakan untuk menyimpan data hendaklah dikawal akses ke atasnya, menilai risiko kehilangan dan maklumat yang mungkin dikompromi serta pelan tindakan bagi mengawal penggunaan bahan-bahan tersebut. Pemilihan kaedah pelupusan yang tepat bagi media elektronik tersebut mampu mengurangkan risiko kehilangan maklumat terhadap pendedahan yang disengajakan, mengurangkan kos operasi, kesan kepada persekitaran dan keputusan yang diambil adalah berpandukan kepada penilaian teknikal yang merangkumi ke semua faktor seperti yang digariskan dalam garis panduan ini.

Justeru itu, Ketua Jabatan hendaklah menentukan supaya arahan-arahan tersebut dipatuhi untuk melindungi aset dan maklumat rahsia rasmi Jabatan daripada sebarang bentuk ancaman keselamatan yang boleh menyusahkan pentadbiran Kerajaan, menjejaskan keselamatan dan kesejahteraan negara.

LAMPIRAN A

MATRIX SANITASI MEDIA ELEKTRONIK

KATEGORI MEDIA ELEKTRONIK	CONTOH MEDIA ELEKTRONIK	RAHSIA BESAR & RAHSIA		SULIT & TERHAD		CATATAN
		SANITASI LOGIKAL	SANITASI FIZIKAL	SANITASI LOGIKAL	SANITASI FIZIKAL	
Peranti Mudah Alih	1. PDA	X	√	√	√	
	2. Tablet	X	√	√	√	
	3. Smartphone dan seumpamanya	X	√	√	√	
Peralatan Rangkaian	1. Router 2. Firewall 3. Web Application Firewall 4. UMTS dan seumpamanya	X	√	√	√	*Reset to Factory Setting*
Embedded Device	1. Mesin Faks 2. Mesin Pencetak 3. Mesin Fotostat 4. GPS 5. SmartTV 6. Biometric Devices 7. IPod dan seumpamanya	X	√	√	√	
Disk Magnetic	1. Floppy Disk 2. Hard Disk 3. Cassette Tapes 4. Tape Drive 5. ZIP Disk dan seumpamanya	X	√	√	√	
Optical Disks	1. CD/DVD 2. CD-RW/DVD-RW dan seumpamanya	X	√	√	√	
Memory	1. Compact Flash Drives, 2. SD Card 3. RAM 4. FPGA Devices 5. Flash Card dan seumpamanya	X	√	√	√**	
Removeable Media	1. USB Flash Drives, 2. External Storage	X	√	√	√	
Smart Card	1. Smart Card, 2. Token	X	√	√	√	
Nota:	X : tidak boleh dilaksanakan √ : cadangan minimum kaedah sanitasi media elektronik yang dibenarkan					
Petunjuk	** sekiranya boleh diaplikasikan					

LAMPIRAN B

[Subperaturan 6(2)]
Borang 3

Arkib 3/08

BORANG PERMOHONAN BAGI PEMUSNAHAN REKOD ELEKTRONIK

<table>
<tr><td colspan="2">BUTIR-BUTIR JABATAN</td><td rowspan="5">Untuk Kegunaan Arkib Negara

Tarikh Terima:</td></tr>
<tr><td>(1) Kementerian/Jabatan/Agensi:</td><td>(2) Bahagian/Cawangan/Unit:</td></tr>
<tr><td colspan="2">(3) Alamat:</td></tr>
<tr><td>(4) Pewujud Rekod
[Jika tidak sama dengan (1)]:</td><td>(5) Telefon:</td></tr>
<tr><td>(6) No. Faksimili:</td><td>(7) Alamat e-mel:</td></tr>
<tr><td colspan="3">MAKLUMAT MENGENAI REKOD</td></tr>
<tr><td colspan="3">(8) Nama dan No. Jadual Pelupusan Rekod:
(9) Tajuk Siri:
(10) Sistem Aplikasi:
(11) Format Rekod:
(12) Jumlah/Saiz dalam Bit:
(13) Jenis Media:
(14) Jumlah Unit Media:
(15) Tarikh Diliputi:
(16) Peringkat Keselamatan:
(17) Lokasi Rekod:
(18) Sebab Pelupusan:
(19) Tempoh Pengekalan Yang Ditentukan Dalam Jadual:
(20) Perihal Rekod:
[Sila lengkapkan Lampiran]</td></tr>
<tr><td colspan="3">(21) Mengikut Seksyen 25 dan 26, Akta Arkib Negara 2003 [Akta 629], saya mengemukakan permohonan ini bagi pemusnahan rekod di atas:

Nama Pegawai: Tandatangan dan Meterai/Cap Jabatan:

Jawatan: Tarikh:</td></tr>
</table>

[Subperaturan 6(2)]
Borang 4

Kewangan-Arkib 4/08

BORANG PERMOHONAN BAGI PEMUSNAHAN REKOD KEWANGAN DAN PERAKAUNAN

BUTIR-BUTIR JABATAN	
(1) Kementerian/Jabatan/Agensi :	(2) Bahagian/Cawangan/Unit:

MAKLUMAT MENGENAI REKOD

(3) Bil.	(4) Tajuk Siri	(5) Tahun Diliputi		(6) Tempoh Pengekalan Yang Ditentukan Dalam Jadual.	(7) Meter Panjang Rekod
		Daripada	Kepada		
					Jumlah Meter Panjang Rekod:

(8) Mengikut Seksyen 25 dan 26 Akta Arkib Negara 2003 [*Akta 629*] dan Arahan Perbendaharaan 150, saya mengemukakan permohonan ini bagi pemusnahan rekod di atas.

Nama Pegawai: **Tandatangan dan Meterai/Cap Jabatan:**
Jawatan: **Tarikh:**

[Peraturan 9(2)]

Borang 12

Arkib 12/08

PENENTUSAHAN PEMUSNAHAN REKOD AWAM

BUTIR-BUTIR JABATAN	
(1) Kementerian/Jabatan/Agensi:	(2) Bahagian/Cawangan/Unit:
MAKLUMAT MENGENAI REKOD	
(3) Surat Kebenaran Pemusnahan: (3.1) No. Rujukan: (3.2) Tarikh:	
(4) Perihal Rekod:	
(5) Meter Panjang Rekod Yang Dimusnahkan:	
(6) Peringkat Keselamatan:	
(7) Kaedah Pemusnahan : No Resit (Jika Dijual):…….. ☐ dibakar ☐ dirincih ☐ dikitar semula ☐ dipadamkan ☐ dijual	
(8) Tarikh Pemusnahan:	(9) Tempat Pemusnahan:
PEGAWAI YANG MELAKSANAKAN PEMUSNAHAN	
(10) Nama Pegawai: Tandatangan: Jawatan:	(11) Nama Saksi: Tandatangan: Jawatan:
PENENTUSAHAN	
(12) Saya mengesahkan bahawa rekod di atas telah dimusnahkan dengan sewajarnya mengikut Seksyen 25 dan 26, Akta Arkib Negara 2003 [*Akta 629*]: Nama Pegawai: Tandatangan dan Meterai/Cap Jabatan: Jawatan: Tarikh:	

[Peraturan 9(2)]

Borang 13

Kewangan-Arkib 13/08

PENENTUSAHAN PEMUSNAHAN
REKOD KEWANGAN DAN PERAKAUNAN

BUTIR-BUTIR JABATAN	
(1) Kementerian/Jabatan/Agensi :	(2) Bahagian/Cawangan/Unit:
MAKLUMAT MENGENAI PEMUSNAHAN	
(3) Kelulusan bagi Pemusnahan • Arkib Negara, No. Rujukan : Tarikh: • Audit Negara, No. Rujukan : Tarikh: • Akauntan Negara No. Rujukan: Tarikh:	
(4) Meter Panjang Rekod Yang Dimusnahkan:	
(5) Kaedah Pemusnahan (tandakan) : ☐ dibakar ☐ dirincih ☐ dikitar semula ☐ dipadamkan ☐ dijual	(6) No Resit (Jika Dijual):……....
(7) Tarikh Pemusnahan :	(8) Tempat Pemusnahan:
PEGAWAI YANG MELAKSANAKAN PEMUSNAHAN	
(9) Nama Pegawai: Tandatangan : Jawatan:	(10) Nama Saksi: Tandatangan : Jawatan :
PENENTUSAHAN	
(11) Saya mengesahkan bahawa rekod di atas telah dimusnahkan dengan sewajarnya mengikut Seksyen 25 dan 26, Akta Arkib Negara 2003 [*Akta 629*] dan Arahan Perbendaharaan 150 Nama Pegawai: Tandatangan dan Meterai/Cap Jabatan: Jawatan: Tarikh:	

LAMPIRAN C

BORANG KPKK/BKICTRR-01/2022

BORANG KEBENARAN SANITASI MEDIA ELEKTRONIK

BUTIR-BUTIR JABATAN	
(1) Kementerian/Jabatan/Agensi:	(2) Bahagian/Cawangan/Unit:

MAKLUMAT MENGENAI MEDIA ELEKTRONIK

(3) Bil.	(4) Rujukan Fail	(5) Perkara	(6) No Siri Media Elektronik	(7) Musnah / Simpan

(8) Pengelasan (tandakan)

☐ Rahsia Besar ☐ Rahsia ☐ Sulit ☐ Terhad ☐ Terbuka

(9) Catatan :

PERAKUAN JAWATANKUASA SANITASI MEDIA ELEKTRONIK

(10) Saya selaku Pengerusi Jawatankuasa Sanitasi Media Elektronik ..... dengan ini memperakui bahawa perkara rahsia rasmi di atas boleh dilupuskan / dimusnahkan mengikut cara-cara yang telah ditetapkan di dalam Arahan Keselamatan (Semakan dan Pindaan 2017) dan peraturan-peraturan berkaitan yang sedang berkuatkuasa.

Nama Pegawai: Tandatangan dan Meterai/Cap Jabatan:

Jawatan: Tarikh:

LAMPIRAN D

BORANG KPKK/BKICTRR-02/2022

BORANG MAKLUMAT SANITASI MEDIA ELEKTRONIK

BUTIR-BUTIR JABATAN	
(1) Kementerian/Jabatan/Agensi :	(2) Bahagian/Cawangan/Unit:
MAKLUMAT MENGENAI PEMUSNAHAN	
(3) Tarikh Pemusnahan :	(4) Tempat Pemusnahan:
(5) Kaedah Sanitasi (Tandakan) ☐ Sanitasi Logikal ☐ Sanitasi Fizikal (6) Catatan :	
PERAKUAN PEGAWAI YANG MELAKSANAKAN	
(7) Adalah dengan ini disahkan bahawa sanitasi media elektronik telah dilaksanakan mengikut proses-proses yang telah ditetapkan seperti garis panduan ini dan berpandukan kepada peraturan dan arahan yang berkuat kuasa. Nama Pegawai: Tandatangan: Jawatan: Tarikh:	
VALIDASI PIHAK KETIGA	
(8) Berdasarkan semakan adalah disahkan bahawa data,maklumat dan rekod rasmi / rahsia rasmi di dalam media elektronik telah dilupuskan dan tidak boleh diperoleh semula dengan apa jua cara. Nama Pegawai: Tandatangan: Jawatan: Tarikh:	

LAMPIRAN E

SIJIL PENGESAHAN SANITASI MEDIA ELEKTRONIK RASMI /RAHSIA RASMI JABATAN

BUTIR-BUTIR JABATAN	
(1) Kementerian/Jabatan/Agensi :	(2) Bahagian/Cawangan/Unit:

PERAKUAN KETUA JABATAN

(3) Saya mengesahkan bahawa suratan/maklumat/bahan rasmi/rahsia rasmi seperti di Lampiran C, Borang Kebenaran Sanitasi Media Elektronik:

☐ telah mematuhi peraturan pengelasan semula mengikut seksyen 2C, Akta Rahsia Rasmi 1972

dan

☐ dimusnahkan dengan sewajarnya mengikut Arahan Keselamatan (Semakan dan Pindaan 2017) dan peraturan-peraturan berkaitan yang sedang berkuatkuasa.

Nama Pegawai:
Jawatan:

Tandatangan dan Meterai/Cap Jabatan:
Tarikh:

DISAHKAN OLEH:

PEJABAT KETUA PEGAWAI KESELAMATAN KERAJAAN MALAYSIA

(4) Saya mengesahkan bahawa sanitasi media elektronik yang menyimpan maklumat rasmi / rahsia rasmi di atas telah dilaksanakan sewajarnya mengikut kehendak Akta Rahsia Rasmi 1972, Arahan Keselamatan (Semakan dan Pindaan 2017), dan peraturan-peraturan berkaitan yang sedang berkuat kuasa.

Nama Pegawai:
Jawatan:

Tandatangan dan Meterai/Cap Jabatan:
Tarikh:

LAMPIRAN F

SENARAI SEMAK AKTIVITI PEMUSNAHAN/SANITASI

Sila tandakan ☑ pada ruangan yang berkenaan :

PERKARA	RUJUKAN / BORANG	YA	TIDAK
Adakah Jawatankuasa Menyemak, Menilai dan Mengelaskan Semula Rahsia Rasmi dibentuk bagi menilai, menyemak dan membuat keputusan bagi melaksanakan sanitasi media elektronik?	**Akta Rahsia Rasmi 1972** Pengelasan semula maklumat rahsia rasmi yang terkandung di dalam media elektronik selaras dengan peruntukan Akta Rahsia Rasmi 1972 [*Akta 88*]. Jika YA : Sila semak dan lengkapkan Buku Daftar Suratan Rahsia Rasmi Am 492/ Am492B	☐	☐
	Borang pengelasan semula mengikut Seksyen 2C, Akta 88 dan Surat Pekeliling Am Bil.2 Tahun 1987. Jika YA : Sila kemukakan dokumen sokongan yang berkaitan.	☐	☐
Adakah proses sanitasi dijalankan mengikut cara-cara yang telah ditetapkan?	**Arahan Keselamatan (Semakan dan Pindaan 2017)** **Lampiran C**: **Borang Kebenaran Sanitasi Media Elektronik**	☐	☐
Adakah proses sanitasi media elektronik perlu melaksanakan Jadual Pelupusan Rekod?	**Akta Arkib Negara 2003** Rekod-rekod elektronik yang hendak dilupuskan perlu disenaraikan seperti di **Lampiran B**: **Borang Permohonan Bagi Pemusnahan Rekod Elektronik**	☐	☐

	Borang 3 [Subperaturan 6(2)] Arkib 3/08.	☐	☐
	Borang 4 [Subperaturan 6(2)] Arkib 4/08.	☐	☐
	Borang 12 [Subperaturan 9(2)] Arkib 12/08.	☐	☐
	Borang 13 [Subperaturan 9(2)] Arkib 13/08.	☐	☐
Adakah Jabatan/Agensi mematuhi peraturan-peraturan yang termaktub di dalam Tatacara Pengurusan Aset Alih Kerajaan?	**Surat Pekeliling Perbendaharaan Bil. 5/2007 (Tatacara Pengurusan Aset Alih Kerajaan).**	☐	☐
	Sijil Penyaksian Pemusnahan Aset Alih Kerajaan KEW.PA-18. Jika YA : Sila kemukakan dokumen sokongan yang berkaitan.	☐	☐
	Sijil Pelupusan Kewangan KEW.PA-19. Jika YA : Sila kemukakan dokumen sokongan yang berkaitan.	☐	☐
Adakah proses sanitasi media elektronik melibatkan pemusnahan secara fizikal yang dikendalikan oleh pihak Jabatan mahupun pihak ketiga?	*Guidelines for Classification of Used Electrical and Electronic Equipment in Malaysia - Department of Environmental (DOE)*. Jika YA : Sila kemukakan dokumen sokongan yang berkaitan.	☐	☐

Adakah proses sanitasi media elektronik melalui validasi oleh pihak ketiga?	**Lampiran D: Borang Maklumat Sanitasi Media Elektronik** Jika YA : Sila kemukakan dokumen sokongan yang berkaitan.	☐	☐
Adakah proses sanitasi media elektronik telah disahkan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia?	**Lampiran E: Sijil Pengesahan Sanitasi Media Elektronik.** Jika YA : Sila kemukakan dokumen sokongan yang berkaitan.	☐	☐
Adakah proses keseluruhan sanitasi media elektronik didokumenkan?	Dokumen-dokumen yang berkaitan dikumpulkan dan difailkan. Jika YA : Sila kemukakan dokumen sokongan yang berkaitan.	☐	☐