



**GARIS PANDUAN PENGURUSAN RAHSIA RASMI
UNIVERSITI KEBANGSAAN MALAYSIA**

**BAHAGIAN GOVERNAN DAN PENTADBIRAN, JABATAN PENDAFTAR
JAWATANKUASA KERJA PEMBANGUNAN GARIS PANDUAN PENGURUSAN
RAHSIA RASMI
UNIVERSITI KEBANGSAAN MALAYSIA
2017**

Isi Kandungan	Muka surat
1.0 Tujuan	1
2.0 Latar Belakang	1
3.0 Peraturan Berkaitan	2
4.0 Tafsiran	2-5
5.0 Terma & Istilah	6-7
6.0 Prosedur Dokumen Terperingkat	7-14
7.0 Langkah-Langkah Mengelaskan Dokumen Dalam Persekitaran ICT	15-16
8.0 Langkah-Langkah Pengelasan Semula Dokumen Rahsia Rasmi Dalam Persekitaran ICT	18-24
9.0 Proses Naik Taraf Dokumen/Fail	25
10.0 Penyimpanan Maklumat Rahsia Rasmi	26
11.0 Penghantaran Maklumat Rahsia Rasmi	26
12.0 Pelepasan Maklumat Rahsia Rasmi	27
13.0 Pelupusan/ Pemusnahan	28-29
14.0 Dasar Kriptografi Negara	29
15.0 Tanggungjawab	29-31
 RAJAH	
Rajah 1 : Carta Alir Pengelasan Rahsia Rasmi	17
Rajah 2 : Carta Alir Pengelasan Semula	25

LAMPIRAN

Lampiran A – Contoh Kulit Fail Dokumen Terperingkat	32
Lampiran B – Borang daftar Klasifikasi/Modul Rahsia Rasmi Secara Elektronik	33-34
Lampiran C – Borang Daftar Klasifikasi Maklumat Rahsia Rasmi Elektronik	35-36

GARIS PANDUAN PENGURUSAN RAHSIA RASMI UNIVERSITI KEBANGSAAN MALAYSIA

1. TUJUAN

Garis panduan ini disediakan adalah sebagai satu sumber rujukan dan panduan kepada warga Universiti Kebangsaan Malaysia (UKM) yang terlibat dengan pengurusan dan penggunaan dokumen rahsia rasmi (fizikal dan elektronik) di UKM.

2. LATAR BELAKANG

- 2.1 Garis panduan ini adalah disediakan berdasarkan undang-undang, pekeliling dan arahan Kerajaan berkaitan mengenai peraturan-peraturan kawalan keselamatan perlindungan untuk UKM.
- 2.2 Berdasarkan Arahan Keselamatan (Semakan dan Pindaan 2017), penetapan darjah keselamatan adalah mengikut prinsip-prinsip tertentu untuk dilaksanakan oleh semua pegawai awam mengikut peruntukan Akta Rahsia Rasmi 1972 [Akta 88] bagi mengawal rahsia-rahsia negara dengan berkesan.
- 2.3 Setiap pegawai awam yang diamanahkan dengan dokumen rahsia rasmi dikehendaki mematuhi peruntukan-peruntukan yang terkandung di dalam Arahan Keselamatan (Semakan dan Pindaan 2017).
- 2.4 Selaras dengan Arahan Keselamatan tersebut, hanya warga UKM yang telah menandatangani borang perakuan dibawah Akta Rahsia Rasmi 1972 [Akta 88] dan lulus tapisan keselamatan sahaja yang dibenarkan menguruskan dokumen rahsia rasmi.

3. PERATURAN BERKAITAN

- Akta Rahsia Rasmi 1972 [Akta 88]
- Akta Arkib Negara 2003
- Akta Tandatangan Digital (1997)
- Akta Perlindungan Maklumat Peribadi (PDPA)
- Arahan Keselamatan
- Arahan/ Pekeliling MAMPU
- Dasar Keselamatan ICT MAMPU
- Dasar Pengurusan Rekod dan Arkib Elektronik (Arkib Negara)

- Dasar Keselamatan ICT UKM
- Dasar Kriptografi Negara
- Rangka Kerja Keselamatan Siber Sektor Awam 2016 (MAMPU)

4. TAFSIRAN

4.1 “Perkhidmatan awam” seperti yang ditafsir di dalam Akta Rahsia Rasmi 1972:

- (a) mana-mana perkhidmatan awam yang disebut dalam Perkara 132 Perlembagaan termasuk sesuatu Kementerian, sesuatu jabatan Kerajaan, atau sesuatu Mahkamah;
- (b) sesuatu majlis bandar raya, perbandaran, majlis bandaran atau pihak berkuasa tempatan;
- (c) sesuatu pihak berkuasa berkanun yang menjalankan kuasa yang terletak hak padanya menurut undang-undang persekutuan atau Negeri;
- (d) mana-mana orang, tribunal, badan, institusi atau pihak berkuasa yang diisytiharkan oleh Menteri dengan perintah yang disiarkan dalam Warta sebagai suatu perkhidmatan awam bagi maksud takrif ini; dan
- (e) sekiranya berlaku peperangan, sesuatu jabatan kerajaan bagi sesuatu negeri sekutu Malaysia.

4.2 “**Rahsia rasmi**” ertinya dokumen atau surat rasmi yang mengandungi maklumat rasmi yang mesti diberi perlindungan untuk kepentingan keselamatan dan bertanda dengan sesuatu peringkat keselamatan. Maklumat dalam dokumen rahsia rasmi mesti diberi perlindungan keselamatan berdasarkan undang-undang berkaitan dan Arahan Keselamatan yang bertujuan untuk mengawal rahsia-rahsia negara dengan berkesan.

4.3 Surat, maklumat atau bahan boleh dikelaskan sebagai Rahsia Besar, Rahsia, Sulit atau Terhad berpandukan Arahan Keselamatan (Semakan dan Pindaan 2017) adalah seperti tafsiran berikut:

- (a) “**Rahsia Besar**” ertinya dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada

Malaysia;

- (b) **“Rahsia”** ertinya 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;
- (c) **“Sulit”** ertinya 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; dan
- (d) **“Terhad”** ertinya dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan *Rahsia Besar*, *Rahsia* atau *Sulit* tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan.

4.4 Apa-apa perkara dinyatakan di bawah Jadual Akta Rahsia Rasmi 1972 adalah seperti berikut:

Suratan, rekod keputusan dan pertimbangan Jemaah Menteri termasuklah juga suratan, rekod keputusan dan pertimbangan jawatankuasa-jawatankuasa Jemaah Menteri;

- (a) Suratan, rekod keputusan dan pertimbangan Majlis Mesyuarat Kerajaan Negeri termasuklah juga suratan, rekod keputusan dan pertimbangan jawatankuasa-jawatankuasa Majlis Kerajaan Negeri; dan
- (b) Suratan berkenaan dengan keselamatan negara, pertahanan dan perhubungan antarabangsa.

4.5 Huraian mengenai keselamatan negara, pertahanan dan perhubungan antarabangsa adalah dihuraikan mengikut perkara-perkara berikut:

(a) **Keselamatan Negara**

Apa-apa maklumat yang berkenaan dengan mana-mana agensi atau jabatan yang terlibat dalam operasi atau aktiviti-aktiviti keselamatan negara termasuklah apa-apa perkara yang berhubung dengan sifat kerjanya yang terselindung,

pengekalan keamanan dan keharmonian, pembelian, modus operandi, pengagihan bantuan teknik serta juga maklumat yang berhubung dengan kertas-kertas penyiasatan yang serius dan sensitif sifatnya yang, jika tidak dilindungi, akan menyentuh kesentosaan negara.

(b) **Pertahanan**

Pertahanan termasuklah:-

- i. saiz, bentuk, susunan, logistik, perintah tempur, pengagihan, operasi, keadaan bersedia dan latihan Angkatan Tentera Malaysia;
- ii. senjata, stor atau kelengkapan lain angkatan itu dan pereka ciptaan, pembangunan, pengeluaran dan pengendalian kelengkapan itu serta penyelidikan yang berhubung dengannya;
- iii. dasar dan strategi pertahanan serta perancangan dan perisikan ketenteraan;
- iv. rancangan-rancangan dan langkah-langkah bagi penyenggaraan bekalan-bekalan dan perkhidmatan-perkhidmatan penting yang diperlukan atau mungkin akan diperlukan semasa peperangan.

(c) **Perhubungan Antarabangsa**

Hubungan antarabangsa ertinya hubungan antara negara, antara organisasi antarabangsa atau di antara satu atau lebih negara dengan satu atau lebih organisasi sedemikian dan termasuklah apa-apa perkara yang berhubung dengan sesuatu negara selain daripada Malaysia atau sesuatu organisasi antarabangsa yang berupaya menyentuh hubungan Malaysia dengan sesuatu negara lain atau dengan sesuatu organisasi antarabangsa.

5. TERMA & ISTILAH

- (a) **“Pegawai Pengelas”** – ertinya Menteri, Menteri Besar atau Menteri atau Pegawai Awam yang dilantik mengikut Seksyen 2B Akta Rahsia Rasmi 1972 untuk mengelaskan surat rasmi, maklumat rasmi dan bahan rasmi kerajaan.

- (b) **“Sistem Maklumat Universiti”** – Sistem yang mengandungi semua aplikasi berkaitan dengan fungsi utama UKM.
- (c) **“Urus Setia Sistem Aplikasi”** - Pusat Tanggungjawab (PTJ) yang bertanggungjawab menggerakkan pelaksanaan sesuatu sistem aplikasi dan menentukan sebarang perubahan ke atas sistem aplikasi tersebut serta bertanggungjawab ke atas pengwujudan, pengemaskinian dan kesahihan maklumat.
- (d) **“Pengguna”** - Seseorang atau kumpulan orang yang dibenarkan menggunakan kemudahan ICT UKM.
- (e) **“Pembangun Sistem”** – Pasukan Pembangun Sistem yang bertanggungjawab membangun dan menyelenggara sistem aplikasi.
- (f) **“Pentadbir Pangkalan Data”** - Pegawai yang diberikan tanggungjawab terhadap pengurusan pangkalan data.
- (g) **“Pentadbir Sistem”** - Pegawai yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara operasi dan keselamatan pelayan dan data yang disimpan.
- (h) **“Pemilik maklumat/ Pemilik Sistem”** - UKM sebagai organisasi yang memiliki semua sistem aplikasi yang dibangunkan secara dalaman atau perisian yang diperolehi serta maklumat yang dihasilkan melalui sistem aplikasi.

6. TATACARA PENGURUSAN DOKUMEN RAHSIA RASMI

Dalam memastikan keselamatan dan tahap kerahsiaan dokumen rahsia rasmi di premis UKM sentiasa terjaga dan selamat dari sebarang penyalahgunaan oleh pihak tidak bertanggungjawab, pegawai dan anggota UKM perlu mematuhi Arahan Keselamatan (Semakan dan Pindaan 2017) seperti berikut;

- (a) peringkat keselamatan dokumen rahsia rasmi;
- (b) tanda keselamatan dokumen rahsia rasmi;
- (c) tatacara penyimpanan dokumen rahsia rasmi;
- (d) tatacara penghantaran dokumen rahsia rasmi;
- (e) tatacara membawa dokumen rahsia rasmi keluar pejabat;
- (f) tatacara pemusnahan dokumen rahsia rasmi;
- (g) tatacara pengurusan kehilangan dokumen rahsia rasmi; dan

- (h) tatacara pengurusan dokumen rahsia rasmi secara elektronik;

6.1 TATACARA PENGURUSAN DOKUMEN RAHSIA RASMI

- (a) Antara contoh dokumen rasmi, maklumat rasmi dan bahan rasmi yang diperingkatkan RAHSIA BESAR adalah:-
- i. kertas-Kertas Jemaah Menteri yang sangat penting mengenai dasar utama Kerajaan berkaitan perkara-perkara politik dan ekonomi;
 - ii. maklumat-maklumat yang sangat penting mengenai perancangan gerakan dan barisan peperangan angkatan tentera jika berlaku perang;
 - iii. surat-menyurat yang sangat penting dengan Kerajaan negara asing mengenai aspek perdagangan dan pertahanan; dan
 - iv. maklumat lengkap yang sangat penting berkenaan dengan pertubuhan-pertubuhan perisikan Malaysia dan kaedah-kaedahnya.
- (b) Bagi fail RAHSIA BESAR hanya Naib Canselor sahaja dibenarkan untuk menggunakan fail berkenaan. Pengurusan Tertinggi lain yang ingin menggunakannya hendaklah mendapatkan kebenaran bertulis dari Naib Canselor.
- (c) Antara contoh dokumen rasmi, maklumat rasmi dan bahan rasmi yang dipertingkatkan RAHSIA adalah:-
- i. kertas-kertas berkaitan dengan Jemaah Menteri;
 - ii. arahan-arahan untuk perwakilan-perwakilan Malaysia yang membuat perundingan dalam negara asing;
 - iii. maklumat-maklumat mengenai pemasangan-pemasangan tentera; dan
 - iv. maklumat-maklumat mengenai pertubuhan-pertubuhan subversif dan kegiatan-kegiatannya.
- (d) Hanya pegawai Gred 54 dan ke atas sahaja yang dibenarkan mengendalikan fail Rahsia. Bagi pegawai Gred 52 dan ke bawah mereka hendaklah mendapatkan kebenaran bertulis daripada Naib Canselor dan semua pegawai terlibat disenaraikan sebagai Jawatan Keselamatan Berjadual (JKB).

- (e) Antara contoh dokumen rasmi, maklumat rasmi dan bahan rasmi yang diperingkatkan SULIT adalah:-
- i. laporan-laporan perisikan biasa;
 - ii. dokumen-dokumen dan panduan-panduan teknik untuk kegunaan latihan tentera atau polis;
 - iii. maklumat-maklumat yang mungkin membolehkan pendapatan faedah kewangan daripadanya jika didedahkan sebelum masa; dan
 - iv. maklumat-maklumat bagi sebarang urusan pentadbiran yang jika didedahkan mendatangkan kesusahan kepada organisasi atau aib kepada individu tertentu seperti fail peribadi, fail Pengurusan Lembaga Pengarah Universiti (LPU), fail Mesyuarat Ketua-Ketua Bahagian (MKB), fail Mesyuarat Pengurusan Universiti (MPU), fail-fail kes/perundangan dan fail kewangan.
- (f) Antara contoh dokumen rasmi, maklumat rasmi dan bahan rasmi yang diperingkatkan TERHAD adalah:-
- i. buku-buku Jabatan bagi maksud arahan;
 - ii. perintah-perintah dan arahan-arahan biasa Jabatan; dan
 - iii. fail mesyuarat dalaman/ bahagian/ unit.
- (g) Pegawai Gred 41 dan ke atas sahaja yang dibenarkan mengendalikan fail SULIT dan TERHAD dengan kebenaran bertulis daripada Ketua Bahagian/ Timbalan Ketua Jabatan di UKM.
- (h) Mana-mana pegawai selain daripada gred yang telah dinyatakan di atas perlu ditentukan dari semasa ke semasa oleh pihak yang diberikan tanggungjawab.
- (i) Semua dokumen berkaitan Mesyuarat Jemaah Menteri (MJM) sama ada dalam bentuk *hard copy* atau elektronik perlu sentiasa mematuhi peraturan keselamatan yang ditetapkan oleh Urusetia MJM iaitu Bahagian Kabinet, Perlembagaan dan Perhubungan Antara Kerajaan, Jabatan Perdana Menteri.
- (j) Contoh kulit fail dokumen rahsia rasmi adalah seperti di **Lampiran A.**

6.2 TANDA KESELAMATAN DOKUMEN RAHSIA RASMI

(a) Rahsia Rasmi Yang Kekal Terjilid

- i. peringkat keselamatan hendaklah ditanda kepada dokumen rahsia rasmi yang kekal dan teguh berjilid dengan huruf cerai atau dicap huruf besar tidak kurang 7mm di sebelah luar kulit hadapan dan belakang di muka tajuk, di muka surat pertama dan penghabisan; dan
- ii. peringkat keselamatan hendaklah juga ditanda dengan huruf cerai atau dicap dengan huruf besar di penjuru kiri sebelah atas dan di penjuru kanan sebelah bawah di setiap muka yang mengandungi perkara bertulis, bercetak atau bercap.

(b) Rahsia Rasmi Yang Tidak Kekal Terjilid

- i. Menanda peringkat keselamatan dengan huruf besar di penjuru kiri sebelah atas dan di penjuru kanan sebelah bawah tiap-tiap muka surat yang mengandungi perkara bertulis, bercetak atau bercap;
- ii. Peringkat keselamatan hendaklah ditanda kepada dokumen rahsia rasmi yang tidak kekal atau tidak teguh jilid dengan dicap, ditaip atau ditulis dengan huruf besar di penjuru kiri sebelah atas dan di penjuru kanan sebelah bawah tiap-tiap muka surat yang mengandungi perkara bertulis, bercetak atau bercap;
- iii. Peringkat keselamatan hendaklah ditanda kepada gambar, filem dan lukisan rahsia rasmi supaya peringkatnya dapat dilihat pada salinan yang dibuat daripadanya. Sebagai tambahan peringkat keselamatan hendaklah ditanda di sebelah belakang gambar, filem dan lukisan berkenaan;
- iv. Peringkat keselamatan fail rahsia rasmi hendaklah ditanda di sebelah luar kulit hadapan dan belakang. Nombor rujukan fail hendaklah di sebelah luar kulit hadapan dan tajuknya dicatatkan sebelah dalam kulit hadapan; dan
- v. Hanya tajuk fail TERHAD sahaja boleh dicatatkan di sebelah luar kulit hadapan.

6.3 TATACARA PENYIMPANAN DOKUMEN RAHSIA RASMI

- (a) Perkara-perkara rahsia rasmi hendaklah disimpan dalam peti-peti keselamatan yang sewajarnya dengan peringkatnya seperti berikut:
- i. rahsia rasmi yang dikelaskan sebagai “Rahsia Besar” hendaklah disimpan di dalam bilik kebal atau peti besi dipasang dengan kunci tatakira. Dokumen-dokumen yang di dalam tindakan pegawai-pegawai awam boleh disimpan untuk sementara waktu dalam kabinet fail keluli atau almari keluli yang dipasang dengan palang besi berkunci tetapi jika bangunan yang diduduki itu tidak mempunyai kawalan keselamatan rapi, dokumen-dokumen tersebut hendaklah dikembalikan untuk disimpan dalam bilik kebal atau peti besi;
 - ii. rahsia rasmi yang dikelaskan sebagai “Rahsia” hendaklah disimpan sama seperti rahsia rasmi yang dikelaskan sebagai “Rahsia Besar” atau dalam kabinet keluli atau almari keluli yang dipasang dengan palang besi berkunci;
 - iii. dokumen rahsia rasmi SULIT dan TERHAD hendaklah disimpan dalam kabinet keluli atau almari keluli dan untuk simpanan sementara dalam mana-mana peti berkunci yang dibenarkan oleh Pegawai Keselamatan Jabatan;
 - iv. perkara rahsia rasmi yang lain daripada dokumen rahsia rasmi termasuk buangan rahsia rasmi yang belum dilupuskan hendaklah disimpan mengikut peraturan di atas kecuali jika keadaannya tidak membenarkan hendaklah disimpan mengikut peraturan yang dibenarkan oleh Pegawai Keselamatan Jabatan dengan persetujuan Pegawai Keselamatan Kerajaan; dan
 - v. perkara rahsia rasmi jika ditinggalkan untuk jangka waktu yang singkat tanpa ditunggu hendaklah dikunci dan semua tingkap ditutup untuk menghindarkan orang-orang yang tidak dibenarkan daripada dapat memerhati dan memperoleh rahsia rasmi. Jika pejabat ditinggalkan untuk jangka waktu yang panjang tanpa ditunggu misalnya seperti waktu rehat, rahsia rasmi hendaklah dikuncikan di dalam peti-peti keselamatan sewajar dengan peringkat keselamatannya.

6.4 TATACARA PENGHANTARAN DOKUMEN RAHSIA RASMI

- (a) Penghantaran dokumen rahsia rasmi dalam negeri hendaklah mematuhi prosedur berikut:
- i. semua PTj yang menghantar rahsia rasmi hendaklah mendapatkan semula keratan resit akuan terima dengan menggunakan Borang Jadual seperti pada Lampiran 'G' Arahan Keselamatan (Semakan dan Pindaan 2017). Satu borang hendaklah digunakan bagi setiap penerima. Lebih daripada satu rahsia rasmi boleh dicatatkan dalam satu borang dengan syarat semua dokumen itu adalah untuk seorang penerima sahaja. Borang itu hendaklah diisi dalam dua salinan dan salinan yang asal hendaklah dilampirkan bersama-sama dengan rahsia rasmi dan dimasukkan di dalam sampul surat yang pertama. Resit akuan yang telah diterima balik hendaklah dilekatkan kepada salinan Borang Jadual berkenaan dan boleh dilupuskan selepas tempoh enam bulan;
 - ii. salinan Borang Jadual yang dihantar hendaklah disemak pada setiap hari untuk menentukan sama ada resit-resitnya diterima semula. Sekiranya resit akuan tidak diterima dalam tempoh tujuh hari, surat peringatan hendaklah dihantar serentak dengan satu penyiasatan serta-merta dijalankan untuk mengetahui kedudukan dokumen yang dihantar. Sekiranya rahsia rasmi itu didapati tidak diterima dan tiada penjelasan yang memuaskan dari pejabat yang menghantar atau pejabat yang dialamatkan, maka Pegawai Keselamatan Jabatan di kedua-dua jabatan berkenaan hendaklah diberitahu dengan segera. Jika resit akuan terima didapati hilang, pihak yang menerima dokumen itu hendaklah menghantar satu surat akuan penerimaan sebagai ganti kepada resit tersebut;

- iii. rahsia rasmi yang dihantar melalui Peti atau “Sistem Beg Berkunci” dikehendaki menggunakan satu sampul surat sahaja. Sampul tersebut hendaklah ditandakan dengan peringkat keselamatan dan nombor rujukan dokumen berkenaan serta nama dan alamat penerimanya dan dimeterikan dengan meteri atau pelekat keselamatan pejabat yang menghantar;
- iv. rahsia rasmi yang tidak dihantar melalui Peti atau “Sistem Beg Berkunci” hendaklah menggunakan dua lapis sampul surat. Sampul surat sebelah dalam hendaklah ditandakan dengan peringkat keselamatan dan nombor rujukan dokumen berkenaan serta nama dan alamat penerimanya dan dimeterikan dengan meteri atau pelekat keselamatan pejabat yang menghantar. Sampul surat tersebut kemudiannya hendaklah dimasukkan ke dalam sampul surat lain yang bertulis nama dan alamat penerimanya sahaja dan dilekatkan dengan gam; dan
- v. penghantaran dokumen keluar negara hendaklah diuruskan melalui Jabatan Pendaftar UKM.

6.5 TATACARA MEMBAWA DOKUMEN RAHSIA RASMI KELUAR PEJABAT

- (a) Dokumen rahsia rasmi RAHSIA BESAR, RAHSIA, SULIT atau TERHAD yang akan dibawa keluar dari premis UKM hendaklah mendapat kebenaran bertulis daripada Naib Canselor atau Pengurusan Tertinggi.

6.6 TATACARA PENGURUSAN KEHILANGAN DOKUMEN RAHSIA RASMI

- (a) Dokumen rahsia rasmi yang hilang hendaklah dilaporkan dengan segera kepada Pejabat Naib Canselor UKM atau yang akan menyiasat dan mengemukakan laporan kepada Pegawai Keselamatan Kerajaan dalam masa 24 jam.

- (b) Jika dokumen rahsia rasmi tersebut terbukti hilang, Jawatankuasa Tatatertib UKM hendaklah menimbang sama ada tindakan tatatertib diambil atau penyiasatan di bawah Akta Rahsia Rasmi 1972 (Akta 88) perlu dijalankan.
- (c) Laporan ke balai polis yang terdekat hendaklah dibuat sekiranya difikirkan sesuatu kesalahan jenayah telah berlaku.

6.7 TATACARA PEMUSNAHAN DOKUMEN RAHSIA RASMI

- (a) Dokumen rahsia rasmi sama sekali tidak boleh dimusnahkan melainkan mengikut arahan-arahan Kerajaan kecuali jika terdapat arahan-arahan khas pada dokumen tersebut seperti 'Musnahkan Selepas 1hb April 1985' atau 'Minta Kebenaran Pemula Sebelum Dimusnahkan'.
- (b) Apabila dokumen RAHSIA BESAR dimusnahkan, satu siji pemusnahan hendaklah dihantar kepada kuasa pemula dokumen tersebut.
- (c) Rujukan kepada Ketua Pengarah Keselamatan Kerajaan dan Ketua Pengarah Arkib Negara hendaklah dibuat terlebih dahulu oleh pihak UKM di atas segala cadangan pemusnahan dokumen rahsia rasmi.
- (d) Dokumen rahsia rasmi termasuk buangan rahsia rasmi hendaklah dikoyak kecil-kecil atau dirincih dengan menggunakan mesin perincih dan dibakar mengikut peraturan-peraturan selamat di bawah penyeliaan penjawat awam yang dibenarkan. Abunya hendaklah dihancurkan sehingga tidak dikenali lagi.
- (e) Bungan rahsia rasmi hendaklah diberikan perlindungan keselamatan yang sepatutnya sehingga dimusnahkan.
- (f) Rujukan kepada Pegawai Keselamatan Kerajaan hendaklah dibuat bagi lain-lain cara pemusnahan

7. LANGKAH-LANGKAH MENGELASKAN DOKUMEN DALAM PERSEKITARAN ICT

7.1 Pengelasan surat-bahan dan rahsia rasmi dalam persekitaran ICT terbahagi kepada dua keadaan iaitu:

- (a) **Penawanan (*capture*) rekod** – "Rekod rahsia rasmi yang ditawan bagi tujuan penyimpanan/ pemprosesan/

penghantaran/ penerimaan secara digital”.

- (b) **Dokumen rahsia rasmi digital** –”suatu surat rasmi yang dihasilkan dalam bentuk elektronik dimana ia digunakan secara digital ataupun dicetak ke media lain”. Pemula mewujudkan dokumen secara digital sama ada melalui email atau dalam bentuk *spreadsheet*.

7.2. Proses pengelasan dokumen dalam persekitaran ICT perlu melalui peringkat dan langkah-langkah seperti berikut:

(a) Semak

Maklumat rahsia rasmi adalah dimulakan oleh Jabatan sendiri dan Pegawai Pengelas menentukan maklumat tersebut samada di dalam Jadual atau di luar Jadual. Perbezaan kategori dokumen di dalam Jadual dan luar Jadual perlu dinyatakan di tempat yang boleh dirujuk oleh pengguna. Semakan bertujuan untuk mengenalpasti jenis buku daftar yang akan digunakan (Fizikal).

(b) Nilai

Pegawai pengelas boleh menentukan (memilih) peringkat keselamatan Rahsia Besar, Rahsia, Sulit dan Terhad terhadap sesuatu rahsia rasmi yang ditawan.

(c) Penandaan

Memberikan tanda keselamatan pada setiap antara muka (interface) dan juga pada semua janaan dengan ciri-ciri keselamatan yang bersesuaian dengan peringkat keselamatan dan penilaian risiko. Janaan merujuk kepada rekod yang ditawan dari pelbagai sistem/ aplikasi yang biasa yang digunakan. Tanda keselamatan ditanda dengan huruf besar dan *bold* di penjuru kiri sebelah atas dan di penjuru kanan sebelah bawah tiap-tiap muka surat.

(d) Daftar

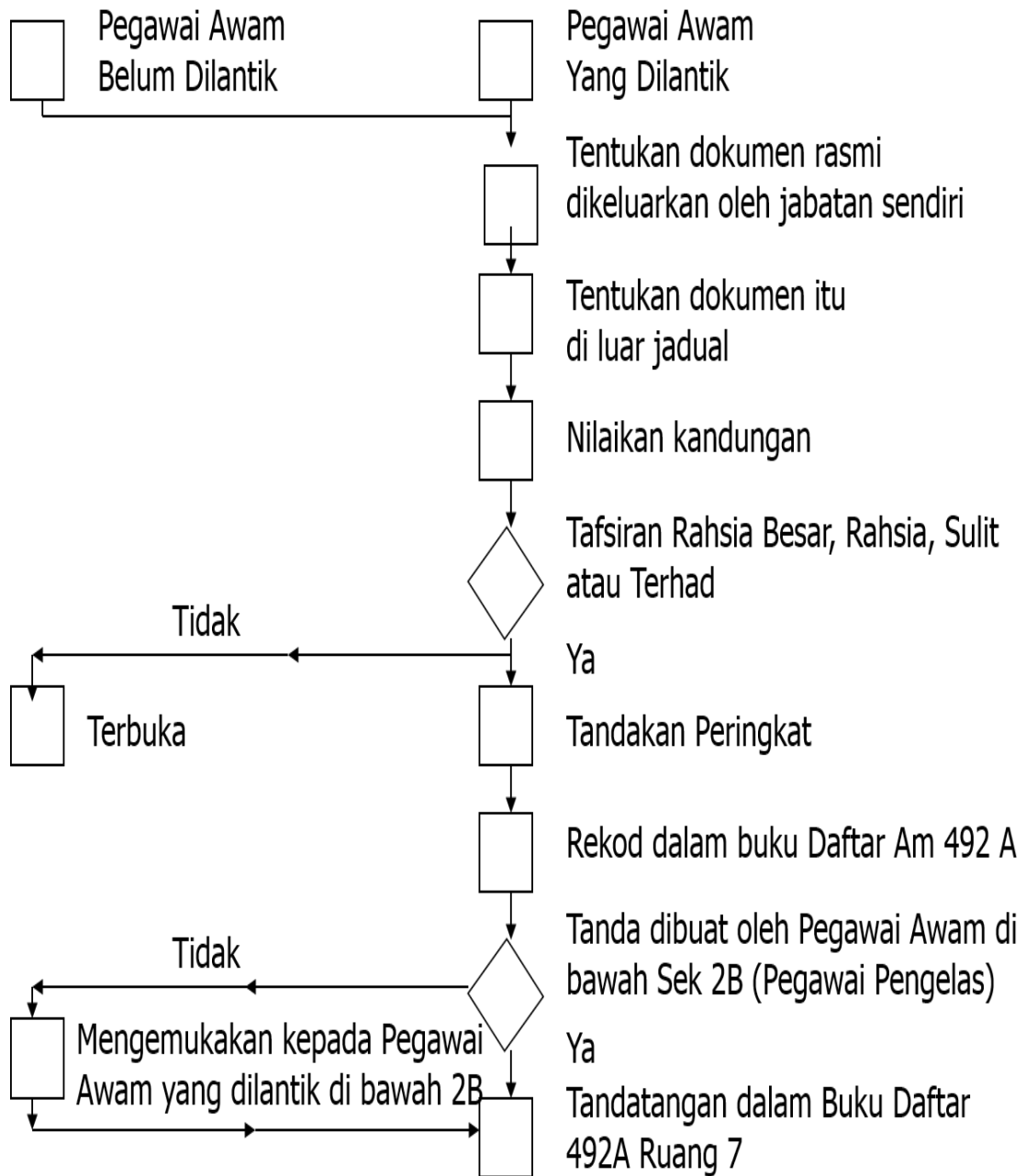
Dokumen rahsia rasmi Dalam Jadual hendaklah didaftarkan dalam Buku Daftar Surat Rasmi AM 492. Manakala dokumen rahsia rasmi Luar Jadual didaftarkan dalam Buku Daftar Surat Rasmi AM 429A dan ditandatangani oleh Pegawai Pengelas (AM 492A sahaja).

(e) Tandatangan

Buku Daftar Suratane Rahsia rasmi dalam persekitaran ICT, Tandatangan Digital hendaklah disediakan untuk Pegawai Pengelasan dan Pegawai Pengelasan Semula (Seksyen 2B dan Seksyen 2C, Akta 88) bagi memenuhi keperluan proses mendaftar Sistem Pendaftaran Suratane Rahsia Rasmi pada buku daftar (AM492, AM492A, AM492B). Tandatangan Digital ini hendaklah sah di sisi undang-undang.

- 7.3. Proses pengelasan dalam persekitaran ICT hendaklah menggunakan borang daftar klasifikasi maklumat dan Borang Daftar Klasifikasi Aplikasi/ Modul. Tatacara penggunaan borang adalah seperti di **Lampiran B dan C**.

CARTA ALIR PENGELASAN RAHSIA RASMI LUAR JADUAL



RAJAH 1.0

8. LANGKAH-LANGKAH PENGELASAN SEMULA DOKUMEN RAHSIA RASMI

8.1 Apa-apa suratan yang dinyatakan dalam jadual atau apa-apa yang telah di luar jadual yang telah dikelaskan akan terhenti menjadi rahsia rasmi selepas pengelasan semula mengikut peruntukan seksyen 2C Akta Rahsia Rasmi 1972 iaitu:

“Seseorang Menteri atau pegawai awam yang dipertanggungjawabkan dengan apa-apa tanggungjawab terhadap 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 boleh, pada bila-bila masa, mengelaskan semula apa-apa suratan yang dinyatakan dalam Jadual atau apa-apa suratan rasmi, maklumat atau bahan sebagaimana yang telah dikelaskan dan selepas pengelasan semula itu, suratan, maklumat atau bahan tersebut hendaklah terhenti menjadi rahsia rasmi.”

8.2 Orang atau pihak yang berkuasa untuk mengelaskan semula dokumen rahsia rasmi ialah:

- (a) Menteri;
- (b) Menteri Besar atau Ketua Menteri;
- (c) Pengelasan Semula oleh Pegawai Awam yang bertanggungjawab terhadap mana-mana Kementerian, Jabatan atau Perkhidmatan Awam (Ketua Setiausaha Negara, semua Ketua Setiausaha, Ketua-Ketua Pengarah dan Jabatan termasuk di peringkat Negeri);
- (d) Ketua Pegawai yang menjaga hal ehwal pentadbiran sesuatu negeri (Y.B. Setiausaha Kerajaan Negeri);
- (e) Ketua Pengurusan/ Ketua Pegawai Eksekutif yang dipertanggungjawabkan menjaga hal ehwal pentadbiran bagi sesuatu Pihak Berkuasa Berkanun atau Syarikat GLC yang menjalankan kuasa yang terletak hak padanya menurut undang-undang persekutuan atau negeri; dan
- (f) mana-mana orang yang diturunkan kuasa oleh Menteri mengikut seksyen 5 Akta Perwakilan Kuasa 1956 (Akta 358) boleh mengelas semula apa-apa suratan yang dinyatakan

dalam jadual atau apa-apa surat rasmi, maklumat atau bahan sebagaimana yang dikelaskan dan selepas pengelasan semula itu Surat, maklumat atau bahan tersebut hendaklah terhenti menjadi rahsia rasmi.

8.3 Sebelum pengelasan semula dibuat surat rasmi disemak bagi menentukan:

- (a) bahawa surat berkaitan dimulakan (*originated*) oleh Jabatan tersebut sahaja;
- (b) bahawa surat berkaitan ialah surat rasmi sama ada dalam Jadual Akta Rasmi 1972 ataupun di luar Jadual; dan
- (c) bahawa kandungan surat berkaitan tidak lagi menyebabkan :
 - i. kerosakan yang amat besar kepada negara; atau
 - ii. membahayakan keselamatan negara; atau
 - iii. keadaan serba-salah kepada kerajaan.

8.4 Selepas pengelasan semula dibuat, surat, maklumat atau bahan tersebut akan terhenti menjadi rahsia rasmi. Berikut adalah tatacara yang mesti dipatuhi dalam pengelasan semula Rahsia Rasmi dan diringkaskan seperti adalah seperti carta alir pada Rajah 1.1:

8.4.1. Pra Pengelasan Semula

- (a) Langkah Pertama - Kuasa Mengelaskan Semula
 - i) Surat, maklumat atau bahan rahsia rasmi hendaklah dikelaskan semula sebagaimana di peruntukan di bawah seksyen 2C Akta Rahsia Rasmi 1972;
 - ii) Seseorang Menteri, Menteri Besar atau Ketua Menteri boleh pada bila-bila masa mengelaskan semula mana-mana dokumen rahsia rasmi di dalam dan luar jadual;

- iii) Pengelasan semula oleh pegawai awam.
Pegawai awam bertanggungjawab terhadap mana-mana. Kementerian, Jabatan dalam Perkhidmatan Awam (Ketua Setiausaha Negara, Semua Ketua Setiausaha Kementerian, Ketua-Ketua Pengarah dan Ketua Jabatan Persekutuan termasuk mana-mana Suruhanjaya di peringkat Persekutuan atau Negeri serta mana-mana jabatan atau agensi di bawah Kerajaan Negeri) boleh pada bila-bila masa mengelaskan semula rahsia rasmi di dalam dan luar jadual;
- iii) Ketua Pegawai yang menjaga hal ehwal pentadbiran sesuatu negeri adalah bermaksud 'Setiausaha Kerajaan Negeri'. Surat rasmi yang diuruskan oleh Kerajaan Negeri boleh dikelaskan semula pada bila-bila masa oleh Setiausaha Kerajaan Negeri; dan
- v) Tindakan pengelasan semula surat, bahan dan maklumat rahsia rasmi hendaklah dijalankan sendiri oleh Menteri/ Pegawai Awam yang berkaitan dan beliau tidak boleh mewakilkan kuasanya bagi melaksanakan tugas tersebut kepada pegawai bawahannya.

(b) Langkah Kedua – Surat, Bahan atau Maklumat

- i) Dokumen, maklumat atau bahan yang hendak dikelaskan semula **MESTI** merupakan milik pemula di Kementerian, Jabatan atau Agensi itu sendiri sahaja.

8.4.2. Semasa Pengelasan Semula

(a) Langkah Pertama - Jawatankuasa Menyemak

- i) Proses pengelasan semula yang hendak dilaksanakan perlulah membentuk satu Jawatankuasa Menyemak yang terdiri daripada mereka yang boleh akses kepada surat, maklumat atau bahan rahsia rasmi.

Pengerusi : Setiausaha Bahagian atau Pengarah Bahagian Pentadbiran

Ahli Jawatankuasa : i. Bahagian Pendaftar Rahsia/
Pendaftar Pejabat;
ii. Pegawai Rekod Kementerian/
Jabatan; dan
iii. Pegawai Keselamatan Kerajaan (Selaku Penasihat)

(Ahli jawatankuasa ini boleh disesuaikan mengikut keperluan Agensi masing-masing)

(b) Langkah Kedua - Penilaian

- i) Penilaian melibatkan kandungan surat rahsia rasmi supaya kandungannya tidak akan menyebabkan kerosakan yang amat besar kepada negara atau tidak membahayakan keselamatan negara ataupun tidak boleh menyebabkan Kerajaan dalam keadaan serba salah.
- ii) Jawatankuasa Menyemak mengemukakan syor mereka kepada Menteri, Menteri Besar, Ketua Menteri, Ketua Jabatan untuk membuat pengelasan semula rahsia rasmi tersebut,

setelah penilaian yang dibuat tidak lagi mendatangkan kesan yang buruk kepada Kerajaan.

(c) Langkah Ketiga - Tempoh Rahsia Rasmi Disemak

- i) Semua suratan, maklumat atau bahan rahsia rasmi yang disemak oleh Jawatankuasa Menyemak bagi sesuatu dokumen tidak ditetapkan tempoh penyemakan sesuatu dokumen harus dilakukan. Ulang kaji ke atas suratan terperingkat hendaklah dilakukan sekurang-kurangnya lima (5) tahun sekali.

(d) Langkah Keempat – Senarai suratan, Maklumat atau Bahan

- i) Pengelasan semula suratan, maklumat atau bahan hendaklah disenaraikan dengan menggunakan format borang pengelasan semula mengikut seksyen 2c akta rahsia rasmi 1972 yang telah disediakan dan ditandatangani oleh mereka yang diberi kuasa di bawah Seksyen 2C Akta Rahsia Rasmi 1972

8.4.3. Selepas Pengelasan Semula

(a) Langkah Pertama - Cop '**TERBUKA**'

- i) Cap Pengelasan Terbuka (Pengelasan Semula) Dokumen yang telah dikelaskan semula diberi penandaan 'Cap Terbuka' tiap-tiap muka surat.

(b) Langkah Kedua - Buku Daftar Rahsia Rasmi Am 492 Di Dalam Jadual dan Berhubung Dengannya atau

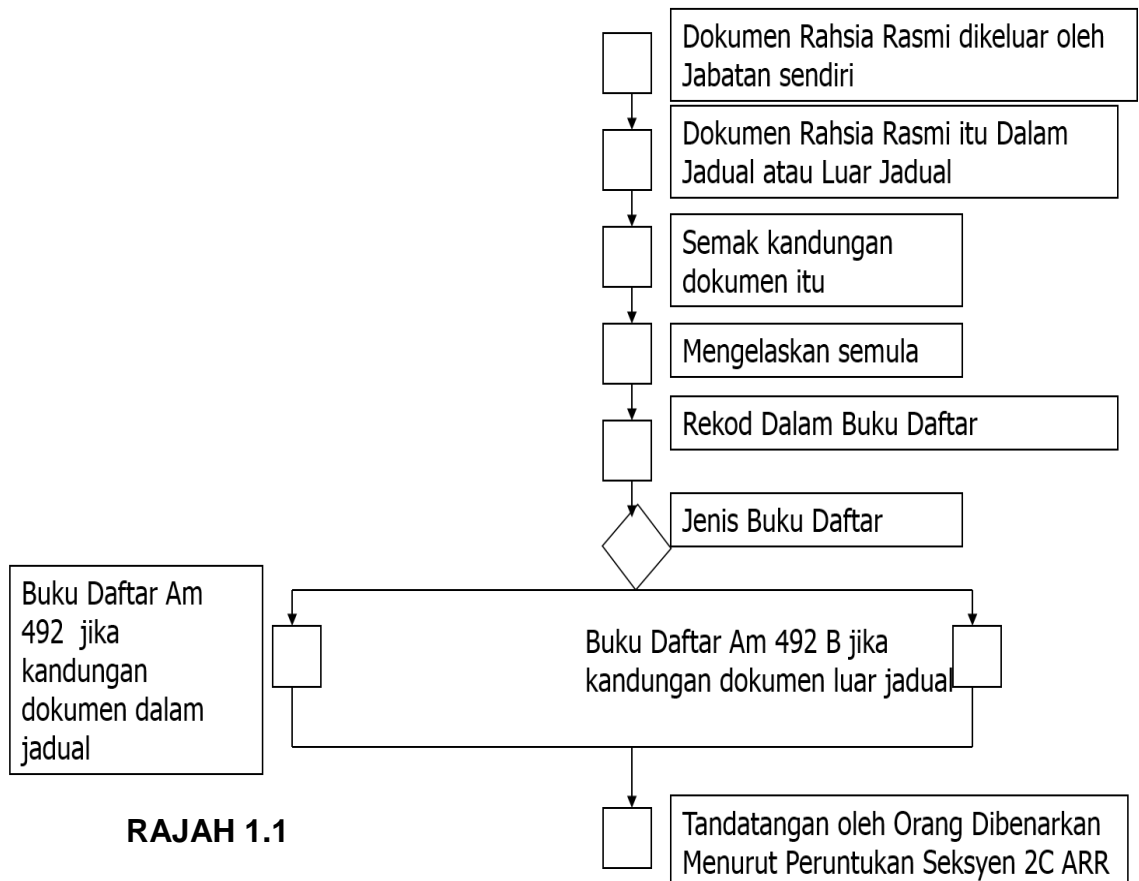
Buku Daftar Rahsia Rasmi Am 492B Di Luar Jadual dan Berhubung Dengannya;

i) Tindakan mendaftar ke dalam Buku Daftar Am 492 atau 492B yang mana berkenaan hendaklah dilaksanakan dan ditandatangani oleh mereka yang diberi kuasa dibawah Seksyen 2C.

(c) Langkah Ketiga - Tanggungjawab Ketua Jabatan;

i) Ketua Jabatan adalah bertanggungjawab memaklumkan kepada Jabatan/Agensi Kerajaan yang mana dokumen,maklumat atau bahan yang dahulunya terperingkat kini telah bertaraf terbuka untuk tindakan selanjutnya Jabatan/Agensi Kerajaan berkenaan.

CARTA ALIR PENGELASAN SEMULA



RAJAH 1.1

9. PROSES NAIK TARAF DOKUMEN/ FAIL

- (a) Bagi proses menaik taraf dokumen atau fail pegawai atau pengguna hendaklah memohon kepada Ketua Jabatan terlebih dahulu. Ketua Jabatan/ Pegawai Pengelas yang memberi kelulusan menaik taraf dokumen/ fail hendaklah memaklumkan melalui memo yang **ditanda** dengan peringkat keselamatan baharu. Dokumen/ fail yang telah dinaik taraf hendaklah diberi rujukan baru dan daftar dalam buku daftar surat rasmi.

10. PENYIMPANAN MAKLUMAT RAHSIA RASMI

- (a) Penyimpanan rasmi dalam persekitaran ICT hendaklah dilindungi secara fizikal dan logikal mengikut perkembangan teknologi dan arahan-arahan Kerajaan dari semasa ke semasa. Pengasingan storan secara fizikal dengan storan yang mengandungi maklumat rasmi. Maklumat Rasmi perlu dienkripsi dengan menggunakan Produk Kriptografi Terpercaya selaras dengan Dasar Kriptografi Negara dan mematuhi mana-mana peraturan yang dikuatkuasakan oleh kerajaan dari masa ke semasa.

11. PENGHANTARAN MAKLUMAT RAHSIA RASMI

- (a) Penghantaran maklumat rasmi melalui peralatan komunikasi hendaklah dibuat melalui kaedah enkripsi dan mematuhi peraturan-peraturan Kerajaan yang dikeluarkan dari semasa ke semasa selaras dengan teknologi semasa. Pergerakan data/ maklumat rasmi didalam sistem hendaklah dilakukan secara khusus (dedicated) dan berasingan dengan maklumat rasmi.
- (b) Semua maklumat Rasmi atas talian perlu berada dalam bentuk teks sifar sepanjang masa, manakala maklumat rasmi yang tidak diperlukan atas talian mesti dipindahkan segera ke media storan elektronik sekunder dalam bentuk teks sifar dan hendaklah dikelaskan.
- (c) Maklumat penerimaan sesuatu dokumen rasmi hendaklah dilaksanakan melalui penggunaan dokumen akuan terima (Borang Jadual). Resit akuan ini bertujuan untuk memastikan dokumen yang dihantar adalah selamat diterima oleh penerima yang sah. Penghantar akan menerima makluman apabila penerima mendapat dokumen tersebut.

12. PELEPASAN MAKLUMAT RAHSIA RASMI

- (a) Rahsia rasmi sama sekali tidak boleh disampaikan ke negara lain tanpa kebenaran Kerajaan Malaysia.
- (b) Keperluan mungkin timbul dari semasa ke semasa untuk menyampaikan rahsia rasmi kepada orang yang bukan dalam perkhidmatan awam sama ada secara lisan atau atas prinsip “Lihat Dan Kembalikan”. Penyampaian rahsia rasmi sedemikian mungkin melibatkan risiko keselamatan dan dalam keadaan itu pegawai-pegawai awam berkenaan dikehendaki:
 - i. menentukan bahawa rahsia rasmi yang minimum sahaja disampaikan;
 - ii. menentukan menerusi saluran-saluran keselamatan bahawa penerima rahsia rasmi boleh dipercayai dan diberi kesedaran di atas keadaan rahsia rasmi itu dan kepentingan menjaganya; dan
 - iii. menentukan bahawa penerima mempunyai persediaan yang cukup untuk menyimpannya dengan selamat.
- (c) Maklumat rahsia rasmi tidak boleh dicapai melalui konsep Bring Your Own Device (BYOD) dan Bring Your Own Environmet (BYOE). (Sehingga kerajaan menetapkan peraturan yang dikuatkuasakan)
- (d) Semua peralatan (device) dan hubungan komunikasi jabatan seperti e-mel rasmi, pesanan segera (instant messaging), persidangan melalui web (web conferencing), perkongsian sumber (shared resources), rangkaian tanpa-wayar (wireless) dan seumpamanya perlu dilindungi daripada capaian yang tidak dibenarkan.

13. PELUPUSAN/ PEMUSNAHAN

- (a) Peralatan yang mengandungi rahsia rasmi dalam persekitaran ICT hendaklah dimusnahkan mengikut peraturan yang ditetapkan oleh Kerajaan dan dilakukan di bawah penyeliaan pegawai awam yang dibenarkan untuk mengendalikan rahsia rasmi tersebut. Semua pemusnahan rahsia rasmi dan peralatannya hendaklah direkodkan.
- (b) Semua maklumat rahsia rasmi hendaklah dimusnahkan termasuk data residue di dalam sistem secara kekal dan buangan rahsia rasmi hendaklah dimusnahkan (rekod rosak / berganda). Pelupusan rahsia rasmi dalam persekitaran ICT perlu melalui sanitasi data mengikut peringkat yang ditetapkan seperti berikut;

(a) Kaedah Sanitasi Data (Rahsia Besar/ Rahsia)

- i. Pemilihan kaedah sanitasi ini hendaklah bergantung kepada kawalan akses ke atas peranti dan media storan. Maklumat ini hendaklah dimusnahkan melalui kaedah sanitasi fizikal dan terdapat tiga (3) kaedah bagi melaksanakan sanitasi tersebut iaitu;
 - a. tulis ganti secara fizikal;
 - b. penyingkiran (purgin); dan
 - c. melaksanakan pemusnahan secara fizikal [perkara Rahsia Besar dan Rahsia] (destroying).
- ii. Semua media yang berupaya menyimpan data adalah hak milik Kerajaan sepenuhnya dan sebarang pemulangan kepada pihak pembekal akibat daripada kerosakan kekal atau perlu ditukar ganti adalah tidak dibenarkan.
- iii. Membuat validasi keselamatan dimana rekod validasi berkenaan pemusnahan rahsia rasmi hendaklah disahkan oleh pihak yang dibenarkan (authorized entity).

(b) Kaedah Sanitasi Data (Sulit/ Terhad)

Maklumat ini hendaklah dimusnahkan melalui kaedah sanitasi logikal. Sanitasi logikal ialah proses menulis ganti (overwrite) data yang berada dalam media elektronik secara logikal. Proses ini hendaklah dilakukan dengan menggunakan perisian yang berupaya melakukan sekurang-kurangnya tiga (3) kali *overwrite* bagi memastikan data benar-benar dipadamkan.

14. DASAR KRIPTOGRAFI NEGARA

Penggunaan Produk Kriptografi Terpercaya adalah mandatori dalam urusan yang melibatkan Rahsia Rasmi. Sebarang penggunaan *Data Encryption Solution* hendaklah mendapat kelulusan Jawatankuasa Dasar Kriptografi Negara.

15. TANGGUNGJAWAB

15.1. Pengurusan Universiti

- (a) Meluluskan Polisi berkaitan Pengurusan Rahsia Rasmi;
- (b) mengesahkan dokumen; dan

- (c) menamakan pegawai pengelas untuk dilantik oleh Menteri Pendidikan Tinggi

15.2. Jawatankuasa Keselamatan Perlindungan UKM

- (a) Rujuk TOR JK yang ditubuhkan

15.3. Ketua Pusat Tanggungjawab (PTj)

- (a) Ketua PTj hendaklah menentukan pelaksanaan kawalan Keselamatan Rahsia Rasmi mengikut Arahan Keselamatan (Pindaan Dan Semakan 2017) berdasarkan perkara-perkara berikut:
 - i. menentukan pelantikan pegawai awam yang layak untuk mengelaskan surat rasmi;
 - ii. melaksanakan pendaftaran surat rasmi yang dikelaskan dan dikelaskan semula dalam Buku Daftar Rahsia Rasmi Am 492 (Di Dalam Jadual dan Berhubung Dengannya), Buku Daftar Rahsia Rasmi 492A (Di Luar Jadual dan Berhubung Dengannya Yang Dikelaskan) & Buku Daftar Rahsia Rasmi 492B (Di Luar Jadual dan Berhubung Dengannya Yang Dikelaskan Semula) mengikut yang mana berkenaan;
 - iii. kesemua buku daftar ini perlu dikawal dan disimpan dengan selamat dan perlu di tender dalam mahkamah sebagai bahan bukti mengenai pengelasan semula rahsia rasmi yang ditetapkan;
 - iv. memaklumkan semua pihak terlibat mengikut surat asal tersebut untuk memaklumkan bahawa surat tersebut telah dikelaskan semula dan terhenti menjadi rahsia rasmi; dan
 - v. menghubungi Pejabat Pegawai Keselamatan Kerajaan bagi mengkaji urusan pengelasan semula atau penurunan taraf peringkat keselamatan dalam persekitaran ICT.

15.4. Jabatan Pendaftar/ Pusat Teknologi Maklumat

- (a) Membangunkan dan menyemak garis panduan pengelasan dokumen rahsia rasmi dari semasa ke semasa.
- (b) Menjalankan aktiviti inspektorat bagi memastikan garis panduan yang berkuat kuasa dipatuhi.

15.5. Pegawai Pengelas

- (a) Menilai dokumen yang perlu dikelaskan

15.6. Urusetia Sistem/ Pembangun Sistem

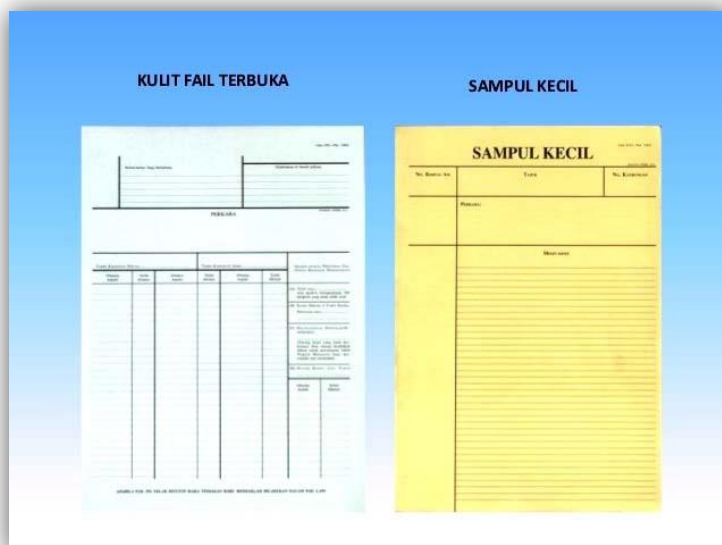
- (a) Memastikan sistem yang dibangunkan mematuhi garis panduan pengurusan maklumat rahsia rasmi.

15.7. Pengguna Sistem

- (a) Mematuhi semua arahan akta rahsia rasmi;
- (b) Perlu memaklumkan sebarang perkara-perkara yang tidak sepatutnya dipaparkan di dalam sistem

LAMPIRAN A

Contoh Kulit Fail Dokumen Rahsia rasmi



LAMPIRAN B

Borang Daftar Aplikasi / Modul						
BORANG DAFTAR KLASIFIKASI APLIKASI / MODUL						
RAHSIA RASMI SECARA ELEKTRONIK						
BUTIR-BUTIR JABATAN						
(1) Kementerian/Jabatan/Agensi:				(2) Bahagian/Cawangan/Unit:		
(3) Alamat:						
(4) Pemula Maklumat [Jika tidak sama dengan (1)]				(5) Telefon:		
(6) No Faksimili:				(7) Alamat e-mel:		
PERIHAL MENGENAI APLIKASI /MODUL						
(8) Tajuk Fail / Nama Fail:						
(9) Format Aplikasi / Modul:						
(10) Jumlah/ Saiz dalam Bit:						
(11) Jenis Media:						
(12) Peringkat / Klasifikasi Aplikasi / Modul:						
(13) Lokasi Aplikasi / Modul:						
(14) Perihal Aplikasi /Modul [Sila lengkapkan]:						
(15) Mengikut Seksyen 2B Akta Rahsia Rasmi 1972 [Akta 88], saya mengelaskan aplikasi / modul di atas mengikut peringkat yang ditentukan:						
Nama Pegawai Pengelas:				Tandatangan dan Meterai/Cap Jabatan:		
Jawatan:				Tarikh:		

PENERANGAN

BORANG DAFTAR KLASIFIKASI APLIKASI /MODUL

(1)	Kementerian/Jabatan/Agensi	Nama Kementerian/Jabatan/Agensi yang memohon
	Contoh:	
	Nama Kem/Jab/Agensi:	Jabatan Perdana Menteri
(2)	Bahagian/Cawangan/Unit:	Bahagian/cawangan/unit yang terdapat dalam sesuatu Kementerian/Jabatan/Agensi yang memohon.
	Contoh:	
	Nama Bhg/Caw/Unit:	Bahagian Khidmat Pengurusan
(3)	Alamat:	Alamat Kementerian/Jabatan/Agensi/Organisasi yang membuat klasifikasi.
(4)	Pemula Maklumat [Jika tidak sama dengan (1)]:	Kementerian/Jabatan/Agensi asal yang mewujudkan atau menguruskan maklumat tetapi fungsi/aktivitinya telah diberhentikan kerana 'jumud' atau fungsinya telah diambilalih oleh jabatan yang baru/lain. Jabatan yang mengambil alih fungsi/aktiviti berkenaan perlu mengisi nama Kementerian/Jabatan/Agensi asal.
(5)	Telefon:	Nombor telefon Kementerian/Jabatan/Agensi/Bahagian/Cawangan/Unit yang membuat klasifikasi
(6)	No. Faksimili:	Nombor faksimili Kementerian / Jabatan / Agensi / Bahagian / Cawangan / Unit yang membuat klasifikasi
(7)	Alamat e-mel:	Alamat e-mel pegawai yang bertanggungjawab
(8)	Tajuk Fail / Nama Fail:	Tajuk / Nama Rujukan Fail yang berkaitan dengan aplikasi / modul yang dibangunkan
(9)	Format Aplikasi / Modul:	Format aplikasi/modul seperti .php, .asp dan sebagainya
(10)	Jumlah/Saiz dalam Bit:	Jumlah/Saiz dalam bit bagi aplikasi/modul yang diklasifikasi
(11)	Jenis Media:	Media storan bagi aplikasi/modul yang diklasifikasi seperti pita magnetik, cd, dvd dan sebagainya
(12)	Peringkat / Klasifikasi Aplikasi / Modul:	Merujuk kepada peringkat pengelasan aplikasi/modul sama ada Terhad, Sulit, Rahsia dan Rahsia Besar.
(13)	Lokasi Aplikasi / Modul:	Merujuk kepada lokasi aplikasi/modul
(14)	Perihal Aplikasi / Modul [Sila lengkapkan]:	Merujuk kepada ringkasan berkaitan aplikasi / modul yang diklasifikasi
(15)	Ruangan ini hendaklah diisi oleh pegawai yang bertanggungjawab membuat klasifikasi	

LAMPIRAN C

									Borang Daftar Maklumat
BORANG DAFTAR KLASIFIKASI MAKLUMAT RAHSIA RASMI ELEKTRONIK									
BUTIR-BUTIR JABATAN									
(1) Kementerian/Jabatan/Agensi:					(2) Bahagian/Cawangan/Unit:				
(3) Alamat:									
(4) Pemula Maklumat [Jika tidak sama dengan (1)]					(5) Telefon:				
(6) No Faksimili:					(7) Alamat e-mel:				
PERIHAL MENGENAI MAKLUMAT									
(8) Tajuk Fail / Nama Fail:									
(9) Format Maklumat:									
(10) Jumlah/ Saiz dalam Bit:									
(11) Jenis Media Storan:									
(12) Peringkat / Klasifikasi Maklumat: TERHAD / SULIT / RAHSIA / RAHSIA BESAR									
(13) Lokasi Maklumat dan Bahan:									
(14) Perihal Maklumat [Sila lengkapkan]:									
(15) Nilai Checksum :									
(16) Mengikut Seksyen 2B Akta Rahsia Rasmi 1972 [Akta 88], saya mengelaskan maklumat di atas sebagai TERHAD / SULIT / RAHSIA / RAHSIA BESAR									
Nama Pegawai Pengelas:					Tandatangan dan Meterai/Cap Jabatan:				
Jawatan:					Tarikh:				

PENERANGAN

BORANG DAFTAR KLASIFIKASI MAKLUMAT

(1)	Kementerian/Jabatan/Agensi: Contoh: Nama Kem/Jab/Agensi: Nama Kem/Jab/Agensi:	Nama Kementerian/Jabatan/Agensi yang membuat Pej. Ketua Pegawai Keselamatan Kerajaan Malaysia Jabatan Perdana Menteri
(2)	Bahagian/Cawangan/Unit: Contoh: Nama Bhg/Caw/Unit: Nama Bhg/Caw/Unit:	Bahagian/cawangan/unit yang terdapat dalam sesuatu Kementerian/Jabatan/Agensi yang membuat klasifikasi Bahagian Khidmat Pengurusan Unit Teknologi Maklumat
(3)	Alamat:	Alamat Kementerian/Jabatan/Agensi/Organisasi yang membuat klasifikasi.
(4)	Pemula Maklumat [Jika tidak sama dengan (1)]: Kementerian/Jabatan/Agensi asal yang mewujudkan atau menguruskan maklumat tetapi fungsi/aktivitinya telah diberhentikan kerana 'jumud' atau fungsinya telah diambilalih oleh jabatan yang baru/lain. Jabatan yang mengambilalih fungsi/aktiviti berkenaan perlu mengisi nama Kementerian/Jabatan/Agensi asal.	
(5)	Telefon:	Nombor telefon Kementerian/Jabatan/Agensi/Bahagian/Cawangan/Unit yang membuat klasifikasi
(6)	No. Faksimili:	Nombor faksimili Kementerian/Jabatan/Agensi/Bahagian/Cawangan/Unit yang membuat klasifikasi
(7)	Alamat e-mel:	Alamat e-mel pegawai yang bertanggungjawab
(8)	Tajuk Fail / Nama Fa	Tajuk / Nama Rujukan Fail yang berkaitan dengan aplikasi / modul yang dibangunkan
(9)	Format Maklumat:	Format maklumat seperti .doc, .jpeg, .xlsx dan sebagainya
(10)	Jumlah/Saiz dalam	Jumlah/Saiz dalam bit bagi maklumat yang diklasifikasi
(11)	Jenis Media:	Media storan bagi maklumat yang diklasifikasi seperti pita magnetik, cd, dvd dan sebagainya
(12)	Peringkat / Klasifikasi Maklumat: Merujuk kepada peringkat pengelasan maklumat sama ada Terhad, Sulit, Rahsia dan Rahsia Besar. Tandakan mana yang berkenaan. Penentuan peringkat keselamatan adalah seperti di Tafsiran dan para 44 Arahan Keselamatan.	
(13)	Lokasi Maklumat:	Merujuk kepada lokasi maklumat disimpan
(14)	Perihal Maklumat [Sila lengkapkan]: Merujuk kepada ringkasan berkaitan maklumat yang diklasifikasi	
(15)	Nilai Checksum : merujuk kepada Hash Value	
(15)	Ruangan ini hendaklah diisi oleh Pegawai Pengelas yang dilantik di bawah Seksyen 2B, Akta Rahsia Rasmi 1972.	