



GARIS PANDUAN PENGURUSAN RAHSIA RASMI

UNIVERSITI MALAYSIA TERENGGANU

**JABATAN GOVERNAN DAN PENGURUSAN PERKHIDMATAN,
PEJABAT PENDAFTAR**

**JAWATANKUASA KERJA PEMBANGUNAN GARIS PANDUAN
PENGURUSAN RAHSIA RASMI**

UNIVERSITI MALAYSIA TERENGGANU

2021

Isi Kandungan

	Muka Surat
1.0 Tujuan	3
2.0 Latar Belakang	3
3.0 Sumber Rujukan	3
4.0 Tafsiran	4
5.0 Pengurusan Rahsia Rasmi	7
6.0 Pengelasan Dokumen Dalam Persekitaran Teknologi Maklumat dan Komunikasi (ICT)	18
7.0 Pengelasan Semula Rahsia Rasmi	23
8.0 Perubahan Peringkat Keselamatan Rahsia Rasmi	27
9.0 Tanggungjawab	28

Rajah

	Muka Surat
Rajah 1 : Carta Alir Pengelasan Semula	30
Rajah 2 : Carta Alir Pengelasan Rahsia Rasmi Luar Jadual	31

Lampiran

	Muka Surat
Lampiran A : Contoh Kulit Fail Dokumen Terperingkat	32
Lampiran B : Borang Jadual	33
Lampiran C : Borang Daftar Klasifikasi Aplikasi / Modul Rahsia Rasmi Secara Elektronik	34
Lampiran D : Borang Daftar Klasifikasi Maklumat Rahsia Rasmi Elektronik	36

GARIS PANDUAN PENGURUSAN RAHSIA RASMI UNIVERSITI MALAYSIA TERENGGANU

1. TUJUAN

Garis panduan ini disediakan sebagai rujukan kepada warga Universiti Malaysia Terengganu (UMT) yang terlibat dalam pengurusan dan penggunaan apa-apa dokumen rahsia rasmi di UMT.

2. LATAR BELAKANG

- 2.1 Garis panduan ini disediakan berdasarkan undang-undang, pekeliling dan arahan Kerajaan mengenai peraturan-peraturan kawalan keselamatan perlindungan yang sedang berkuatkuasa.
- 2.2 Berdasarkan Arahan Keselamatan (Semakan dan Pindaan 2017), penetapan darjah keselamatan adalah mengikut prinsip-prinsip peruntukan Akta Rahsia Rasmi 1972 [Akta 88] bagi mengawal rahsia rasmi Kerajaan dan Universiti dengan berkesan.
- 2.3 Setiap Pegawai Universiti yang diamanahkan dengan dokumen rahsia rasmi dikehendaki mematuhi peruntukan-peruntukan yang terkandung di dalam Arahan Keselamatan (Semakan dan Pindaan 2017).

3. SUMBER RUJUKAN

Sumber rujukan penggubalan garis panduan ini adalah sepertimana berikut:

- (a) Akta Rahsia Rasmi 1972 [Akta 88];
- (b) Akta Arkib Negara 2003 [Akta 629];
- (c) Akta Tandatangan Digital 1997 [Akta 562];
- (d) Akta Perlindungan Data Peribadi 2010 [Akta 709];
- (e) Arahan Keselamatan (Semakan dan Pindaan 2017);
- (f) Pekeliling / Dasar / Arahan MAMPU;

- (g) Dasar Pengurusan Rekod dan Arkib Elektronik (Arkib Negara);
- (h) Dasar Kriptografi Negara (2013);
- (i) Rangka Kerja Keselamatan Siber Sektor Awam 2016 (MAMPU); dan
- (j) Dasar dan Peraturan Teknologi Maklumat dan Komunikasi (ICT) UMT 2016.

4. TAFSIRAN

Dalam garis panduan ini, melainkan jika konteksnya mengkehendaki makna yang lain –

“Dalam Jadual” dengan merujuk Akta Rahsia Rasmi 1972 [Akta 88] bermakna:

- (a) Surat, rekod keputusan, dan pertimbangan Jemaah Menteri termasuk surat, rekod keputusan dan pertimbangan jawatankuasa-jawatankuasa Jemaah Menteri;
- (b) Surat, rekod keputusan dan pertimbangan Majlis Mesyuarat Kerajaan Negeri termasuklah juga surat, rekod keputusan dan pertimbangan jawatankuasa-jawatankuasa Majlis Mesyuarat Kerajaan Negeri; dan
- (c) Surat berkenaan dengan keselamatan negara, pertahanan dan perhubungan antarabangsa;

“Ketua Jabatan” ertinya seseorang pegawai yang bertanggungjawab bagi sesuatu jabatan, bahagian, unit atau cawangan Universiti

“Kuasa asing” ertinya mana-mana negara merdeka dan berdaulat termasuklah mana-mana pertubuhan atau entiti di dalam atau di luar Malaysia sama ada secara langsung atau tidak langsung boleh memudaratkan keselamatan atau kepentingan Malaysia bagi kepentingan suatu negara asing;

“Luar Jadual” adalah apa-apa surat, maklumat dan bahan rasmi yang boleh dikelaskan sebagai ‘Rahsia Besar’, ‘Rahsia’, ‘Sulit’ atau ‘Terhad’ oleh

seorang Menteri, Menteri Besar, Ketua Menteri atau pegawai awam yang dilantik di bawah Seksyen 2B, Akta Rahsia Rasmi 1972.

“Menteri” ertinya Menteri yang dipertanggungjawabkan dengan tanggungjawab bagi pengajian tinggi;

“Naib Canselor” ertinya Ketua Pegawai Eksekutif Universiti dan bertanggungjawab bagi keseluruhan fungsi pentadbiran, akademik dan pengurusan hal ehwal hari ke hari Universiti;

“Pegawai Awam” ertinya seseorang yang memegang sesuatu jawatan atau pekerjaan dalam atau di bawah sesuatu perkhidmatan awam;

“Pegawai Keselamatan Pusat Tanggungjawab” ertinya pegawai yang dilantik oleh PTj yang bertanggungjawab menyelaras dan melaksanakan perkara-perkara yang berkaitan dengan keselamatan perlindungan di PTj masing-masing;

“Pegawai Keselamatan Kerajaan” ertinya pegawai yang dilantik sebagai Pegawai Keselamatan Kerajaan atau mana-mana pegawai yang berkhidmat sebagai Pegawai Keselamatan Kerajaan atau pegawai yang menjalankan tugas sebagai Pegawai Keselamatan Kerajaan;

“Pegawai Pengelas” ertinya Menteri, Menteri Besar atau Menteri atau Pegawai Awam termasuklah Pegawai Universiti yang dilantik mengikut Seksyen 2B Akta Rahsia Rasmi 1972 [Akta 88] untuk mengelaskan surat rasmi, maklumat rasmi dan bahan rasmi Kerajaan atau Universiti;

“Pegawai Universiti” ertinya mana-mana orang yang diambil kerja oleh Universiti di bawah perlembagaan atau mana-mana statut;

“Perkhidmatan awam” adalah termasuk seperti berikut:

- (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.
- (f) mana-mana Pegawai Universiti iaitu mana-mana orang yang diambil kerja oleh UMT di bawah Perlembagaan Universiti atau mana-mana statut;

“Pegawai Keselamatan Jabatan” ertinya pegawai yang dilantik oleh pihak Universiti, bertanggungjawab menyelaras dan melaksanakan perkara-perkara yang berkaitan dengan keselamatan perlindungan di UMT

“Rasmi” ertinya adalah berhubungan dengan perkhidmatan awam;

“Rahsia rasmi” ertinya apa-apa surat yang dinyatakan dalam Jadual Akta Rahsia Rasmi 1972 [Akta 88] dan apa-apa maklumat dan bahan yang berhubungan dengannya dan termasuklah apa-apa surat rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad” mengikut mana-mana yang berkenaan, oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu Negeri atau mana-mana Pegawai Awam yang dilantik di bawah Seksyen 2B Akta Rahsia Rasmi 1972 [Akta 88] untuk mengelaskan apa-apa surat rasmi, maklumat atau bahan sebagai rahsia rasmi;

“Universiti” ertinya Universiti Malaysia Terengganu (UMT);

5. PENGURUSAN RAHSIA RASMI

Pegawai Universiti hendaklah memastikan keselamatan dan tahap kerahsiaan dokumen rahsia rasmi di premis Universiti sentiasa dilindungi dan selamat dari sebarang penyalahgunaan oleh pihak yang tidak bertanggungjawab dan hendaklah mematuhi Arahan Keselamatan (Semakan dan Pindaan 2017) seperti berikut:

5.1 Tatacara Penentuan Peringkat Keselamatan Rahsia Rasmi

Peraturan bagi melindungi keselamatan maklumat adalah ditetapkan mengikut tafsiran semua perkara rahsia rasmi sepertimana berikut:

- (a) peringkat dokumen bergantung kepada kandungan dan bukan peringkat fail. Dokumen di atas perkara yang sama tidak semestinya diberi peringkat yang sama dengan peringkat dokumen yang terdahulu;
- (b) peringkat bagi dokumen tidak bergantung kepada perkara utama. Sesuatu dokumen mungkin mengandungi maklumat rahsia rasmi yang perlu dikelaskan;
- (c) maklumat terkumpul yang diperolehi daripada beberapa dokumen memerlukan peringkat yang lebih tinggi daripada peringkat sesuatu dokumen;
- (d) peringkat dokumen yang mempunyai lampiran mestilah diperingkatkan dengan peringkat lampiran yang tertinggi;
- (e) pemula dokumen hendaklah menentukan kesan sekiranya dokumen dikompromi, sebelum memberi sesuatu peringkat kepada sesuatu dokumen;

- (f) penggunaan peringkat keselamatan yang betul amat penting agar semua peraturan-peraturan dalam penyelenggaraan dan penggunaannya tidak membebankan setiap orang yang terlibat;
- (g) peringkat bagi sesuatu fail tidak boleh rendah daripada peringkat dokumen yang tertinggi sekali yang terkandung dalam sesuatu fail; dan
- (h) peringkat bagi sesuatu fail perlu lebih tinggi daripada peringkat dokumen jika maklumat di dalamnya memerlukan peringkat yang lebih tinggi.

5.2 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 terperingkat 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.

5.3 Kategori Rahsia Rasmi serta Tatacara Penyimpanan

5.3.1 Rahsia Besar

- (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) dokumen rasmi, maklumat rasmi dan bahan rasmi yang diperingkatkan sebagai Rahsia Besar antaranya adalah sepertimana berikut:
 - (i) kertas-kertas Jemaah Menteri yang mengandungi maklumat sangat penting mengenai dasar utama Kerajaan berkaitan perkara-perkara politik atau ekonomi negara;
 - (ii) maklumat-maklumat mengenai perancangan gerakan peperangan dan barisan angkatan tentera jika berlaku perang;

- (iii) surat-menyurat yang mengandungi maklumat sangat penting dengan Kerajaan negara asing mengenai aspek perdagangan dan pertahanan;
 - (iv) maklumat lengkap yang sangat penting berkenaan dengan pertubuhan-pertubuhan perisikan Malaysia dan kaedah-kaedahnya; dan/atau
- (c) Naib Canselor mempunyai akses kepada fail Rahsia Besar. Mana-mana pegawai Pengurusan Tertinggi atau pegawai lain yang ingin mendapatkan akses kepada fail tersebut hendaklah mendapatkan kebenaran bertulis daripada Naib Canselor terlebih dahulu.
- (d) Pegawai-pegawai yang diberi kebenaran untuk mengurus dan mengendalikan dokumen / fail Rahsia Besar hendaklah lulus tapisan keselamatan halus.
- (e) Tatacara Penyimpanan

Rahsia rasmi yang dikelaskan sebagai Rahsia Besar hendaklah disimpan di dalam bilik kebal atau peti besi dipasang dengan kunci tatakira di Pejabat Naib Canselor. Dokumen-dokumen yang di dalam tindakan Pegawai Universiti 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.

5.3.2 Rahsia

- (a) 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 dan/atau Universiti atau memberi keuntungan besar kepada seseorang kuasa asing.

- (b) dokumen rasmi, maklumat rasmi dan bahan rasmi yang diperingkatkan sebagai Rahsia antaranya adalah sepertimana berikut:
 - (i) kertas-kertas berkaitan dengan Jemaah Menteri;
 - (ii) arahan-arahan untuk perwakilan-perwakilan Malaysia dan Universiti yang membuat perundingan dengan negara asing;
 - (iii) maklumat-maklumat mengenai pemasangan-pemasangan tentera;
 - (iv) maklumat-maklumat mengenai pertubuhan-pertubuhan subversif dan kegiatan-kegiatanannya; dan/atau
- (c) mana-mana Ketua Jabatan dibenarkan mengakses fail Rahsia. Manakala pegawai lain yang ingin mendapatkan akses kepada fail tersebut hendaklah mendapatkan kebenaran bertulis daripada Naib Canselor.
- (d) Pegawai-pegawai yang diberi kebenaran untuk mengurus dan mengendalikan dokumen / fail Rahsia hendaklah lulus tapisan keselamatan halus.
- (e) Tatacara Penyimpanan

Rahsia rasmi yang dikelaskan sebagai Rahsia hendaklah disimpan dan diuruskan sama seperti rahsia rasmi yang dikelaskan sebagai Rahsia Besar atau dalam kabinet keluli atau almari keluli yang dipasang dengan palang besi berkunci di Pejabat Naib Canselor atau Pejabat Pendaftar.

5.3.3 Sulit

- (a) Sulit ertinya dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan Malaysia, kegiatan Kerajaan atau Universiti tetapi memudaratkan kepentingan, martabat Malaysia, kegiatan Kerajaan,

Universiti, orang perseorangan atau akan menyebabkan keadaan memalukan, kesusahan kepada pentadbiran atau akan menguntungkan sesebuah pihak luar atau kuasa asing.

(b) dokumen rasmi, maklumat rasmi dan bahan rasmi yang diperingkatkan Sulit antaranya adalah sepertimana berikut:

- (i) laporan-laporan siasatan ;
- (ii) dokumen-dokumen dan panduan-panduan teknik untuk kegunaan keselamatan Universiti;
- (iii) maklumat-maklumat yang mungkin membolehkan pendapatan faedah kewangan daripadanya jika didedahkan sebelum masa;
- (iv) maklumat-maklumat bagi sebarang urusan pentadbiran yang jika didedahkan mendatangkan kesusahan kepada Universiti atau aib kepada Pegawai Universiti tertentu seperti fail Mesyuarat Lembaga Pengarah Universiti (LPU), soalan peperiksaan, fail kes perundangan dan fail kewangan; dan/atau
- (v) apa-apa maklumat lain yang diklasifikasikan sebagai Sulit oleh Pegawai Pengelas.

(c) Pegawai Universiti dibenarkan mengakses fail Sulit dengan kebenaran bertulis daripada Ketua Jabatan masing-masing bagi urusan kerja rasmi dan hendaklah lulus tapisan keselamatan kasar.

(d) Tatacara Penyimpanan

Rahsia rasmi yang dikelaskan sebagai Sulit hendaklah disimpan dalam kabinet keluli atau almari keluli atau bilik berkunci dan untuk simpanan sementara dalam mana-mana tempat berkunci yang dibenarkan oleh Pegawai Keselamatan PTj masing-masing.

5.3.4 Terhad

- (a) 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.
- (b) dokumen rasmi, maklumat rasmi dan bahan rasmi yang diperingkatkan Terhad antaranya adalah sepertimana berikut:
 - (i) buku-buku PTj bagi maksud arahan;
 - (ii) perintah-perintah dan arahan-arahan biasa PTj;
 - (iii) fail mesyuarat dalaman/bahagian/ seksyen/ unit; dan/atau
 - (iv) apa-apa maklumat lain yang diklasifikasikan sebagai Terhad oleh Pegawai Pengelas.
- (f) Pegawai Universiti dibenarkan mengakses fail Terhad dengan kebenaran bertulis daripada Ketua Jabatan masing-masing dan hendaklah lulus tapisan keselamatan kasar.
- (g) Tatacara Penyimpanan

Rahsia rasmi yang dikelaskan sebagai yang dikelaskan sebagai Terhad hendaklah disimpan dalam kabinet keluli atau almari keluli dan untuk simpanan sementara dalam mana-mana peti berkunci yang dibenarkan oleh Pegawai Keselamatan PTj masing-masing.

5.3.6 Panduan penyediaan kulit fail dokumen rahsia rasmi adalah sepertimana di **Lampiran A.**

5.3.7 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 PTj masing-masing dengan persetujuan Pegawai Keselamatan Kerajaan; dan

5.3.8 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 tersebut. Jika pejabat ditinggalkan untuk jangka waktu yang panjang tanpa ditunggu misalnya seperti waktu rehat, rahsia rasmi tersebut hendaklah dikuncikan di dalam peti-peti keselamatan sewajar dengan peringkat keselamatan.

5.4 Tatacara Penghantaran Dokumen Rahsia Rasmi

Penghantaran dokumen rahsia rasmi dalam negeri hendaklah mematuhi prosedur berikut:

- (a) semua PTj yang menghantar rahsia rasmi hendaklah menggunakan Borang Jadual Penghantaran Dokumen Rasmi sepertimana di **Lampiran B**. 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 Penghantaran Dokumen Rasmi berkenaan dan boleh dilupuskan selepas tempoh enam bulan;
- (b) 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 pihak yang menghantar atau pihak yang dialamatkan, maka di kedua-dua pihak 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;

- (c) 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 PTj yang menghantar;
- (d) 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 (sampul kedua) yang bertulis nama dan alamat penerimanya sahaja dan dilekatkan dengan gam; dan
- (e) penghantaran rahsia rasmi ke luar Malaysia hendaklah menggunakan sistem dua lapis sampul surat mengikut peraturan di perkara (d) beserta dengan Borang Jadual Penghantaran Dokumen Rasmi seperti amalan biasa tetapi disematkan di luar sampul surat sebelah dalam. Sampul surat sebelah luar yang dialamatkan kepada Pendaftar Rahsia Kementerian Luar Negeri hendaklah dihantar kepadanya mengikut prosedur yang dibenarkan. Apabila sampul surat sebelah luar dibuka di Kementerian Luar Negeri, sampul surat sebelah dalam hendaklah dihantar mengikut prosedur khas penghantaran Rahsia rasmi kepada penama yang dialamatkan di luar Malaysia. Resit Akuan terima hendaklah dikembalikan kepada pejabat yang menghantar oleh Pendaftar Rahsia, Kementerian Luar Negeri. Penerangan lanjut mengenai prosedur ini boleh didapati daripada Ketua Pengarah Keselamatan Kerajaan atau Pegawai Keselamatan Jabatan, Kementerian Luar Negeri;

- (f) penghantaran Rahsia rasmi ke luar negara hendaklah diuruskan atau diproses melalui Pejabat Pendaftar Universiti; dan
- (g) dokumen Rahsia rasmi yang dihantar secara elektronik perlu disediakan dalam bentuk fail kepilang (*attachment*) dan disulitkan (*encrypted*).

5.5 Tatacara Membawa Dokumen Rahsia Rasmi Keluar Pejabat

- (a) dokumen rahsia rasmi yang dikelaskan sebagai Rahsia Besar dan Rahsia yang dibawa keluar dari premis Universiti hendaklah mendapat kebenaran bertulis daripada Naib Canselor;
- (b) dokumen rahsia rasmi yang dikelaskan sebagai Sulit Atau Terhad yang dibawa keluar dari premis Universiti hendaklah mendapat kebenaran bertulis daripada Ketua Jabatan atau Pegawai Keselamatan PTj masing-masing.

5.6 Tatacara Pengurusan Kehilangan Dokumen Rahsia Rasmi

- (a) dokumen rahsia rasmi yang hilang hendaklah dilaporkan dengan segera kepada Pegawai Keselamatan PTj atau Pegawai Keselamatan Jabatan (Universiti) atau Naib Canselor. Pegawai Keselamatan PTj atau Pegawai Keselamatan Jabatan hendaklah menyiasat dan mengemukakan laporan kepada Naib Canselor berkenaan kehilangan dokumen rahsia rasmi. Naib Canselor kemudiannya hendaklah melaporkan kehilangan dokumen rahsia rasmi tersebut kepada Pegawai Keselamatan Kerajaan dalam masa 24 jam.
- (b) jika dokumen rahsia rasmi tersebut terbukti hilang, bocor atau dimanipulasi, Naib Canselor hendaklah mempertimbangkan sama ada tindakan tatatertib di bawah Akta Badan-Badan Berkanun (Tatatertib & Surcaj) 2000 yang sedang berkuatkuasa 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.

5.7 Tatacara Pemusnahan Rahsia Rasmi

- (a) rahsia rasmi 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) Semua rahsia rasmi Universiti yang akan dimusnahkan hendaklah diselaraskan di peringkat Jawatankuasa Menyemak/Pelupusan Universiti. Tugas utama Jawatankuasa ini adalah untuk menyemak dan menilai sesuatu rahsia rasmi yang akan dilupuskan serta memberi cadangan untuk dikelaskan semula rahsia rasmi kepada Naib Canselor sekiranya maklumat rahsia rasmi tersebut tidak lagi memberi apa-apa implikasi kepada Universiti, Kerajaan atau Negara. Mana-mana rahsia rasmi yang boleh dimusnahkan hendaklah dikelaskan semula terlebih dahulu menjadi 'Terbuka' oleh Naib Canselor. Perincian lanjut adalah seperti di Perenggan 7, Garis Panduan ini.
- (c) apabila Rahsia Besar dimusnahkan, suatu sijil pemusnahan Rahsia Besar hendaklah dikeluarkan terhadap Rahsia Besar tersebut oleh PTj yang membuat pemusnahan. Sekiranya pemula Rahsia Besar itu adalah PTj lain daripada jabatan yang memusnahkan Rahsia Besar tersebut, maka PTj yang membuat pemusnahan terhadap Rahsia Besar itu hendaklah menghantar sijil pemusnahan kepada pemula Rahsia Besar tersebut sebagai makluman. Dalam keadaan terkecuali iaitu peraturan ini tidak dapat dipatuhi misalnya kerana pemula tidak wujud lagi, rujukan kepada Ketua Pengarah Keselamatan Kerajaan hendaklah dibuat sebelum Rahsia Besar tersebut dimusnahkan.

- (d) rujukan kepada Ketua Pengarah Keselamatan Kerajaan dan Ketua Pengarah Arkib Negara hendaklah dibuat terlebih dahulu oleh pihak Universiti di atas segala cadangan pemusnahan dokumen rahsia rasmi.
- (e) 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 Pegawai Universiti atau Pegawai Keselamatan PTj yang dibenarkan. Sisanya hendaklah dihancurkan sehingga tidak dikenali lagi.
- (f) buangan rahsia rasmi hendaklah diberikan perlindungan keselamatan yang sepatutnya sehingga dimusnahkan.
- (g) rujukan kepada Pegawai Keselamatan Kerajaan hendaklah dibuat bagi lain-lain cara pemusnahan.

6. PENGELASAN DOKUMEN DALAM PERSEKITARAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

6.1 Pengelasan suratan bahan dan rahsia rasmi dalam persekitaran ICT terbahagi kepada dua keadaan iaitu:

- (a) **Penawanan (*capture*) rekod**
penawanan rekod ertinya “rekod rahsia rasmi yang ditawan bagi tujuan penyimpanan/ pemprosesan/ penghantaran/ penerimaan secara digital”.
- (b) **Dokumen rahsia rasmi digital**
dokumen rahsia rasmi digital ertinya “suatu suratan rahsia rasmi yang dihasilkan dalam bentuk elektronik di mana ia digunakan secara digital ataupun dicetak ke media lain”.

6.2 Proses pengelasan dokumen perlu melalui peringkat dan langkah-langkah seperti berikut:

(a) **Semak**

maklumat rahsia rasmi adalah dimulakan oleh PTj 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 dokumen rahsia rasmi yang akan digunakan

(b) **Nilai**

Pegawai Pengelas boleh menentukan (memilih) peringkat keselamatan sama ada Rahsia Besar, Rahsia, Sulit dan Terhad terhadap sesuatu rahsia rasmi yang ditawarkan mengikut tafsiran dalam Arahan Keselamatan (Semakan dan Pindaan 2017).

(c) **Penandaan**

memberikan tanda keselamatan pada setiap paparan 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 ditawarkan 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 Dokumen Rahsia Rasmi AM 492. Manakala dokumen rahsia rasmi Luar Jadual didaftarkan dalam Buku Daftar Suratan Rahsia Rasmi AM 429A dan ditandatangani oleh Pegawai Pengelas (AM 492A sahaja).

(e) **Tandatangan**

Pegawai Pengelas hendaklah menurunkan tandatangan di dalam Buku Daftar Am 492A bagi dokumen rahsia rasmi Luar Jadual sahaja.

6.3 Proses pengelasan hendaklah menggunakan Borang Daftar Klasifikasi Maklumat dan Borang Daftar Klasifikasi Aplikasi/ Modul seperti di **Lampiran C dan Lampiran D**.

6.4 Penyimpanan rahsia rasmi 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 hendaklah dibuat. Maklumat rahsia rasmi perlu dienkrp dengan menggunakan Produk Kriptografi Terpercaya selaras dengan Dasar Kriptografi Negara dan mematuhi mana-mana peraturan yang dikuatkuasakan oleh Kerajaan dari semasa ke semasa.

6.5 **Penghantaran Rahsia Rasmi**

- (a) penghantaran rahsia 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 rahsia rasmi didalam sistem hendaklah dilakukan secara khusus (*dedicated*) dan berasingan dengan maklumat rasmi.
- (b) penghantaran rahsia rasmi melalui medium yang tidak selamat sebagai contoh menggunakan aplikasi media sosial seperti *whatsapp*, *telegram*, *instagram* dan seumpamanya adalah dilarang sama sekali. Semua Pegawai Universiti hendaklah menggunakan e-mel rasmi Universiti bagi menghantar dokumen rahsia rasmi dengan kaedah enkripsi.
- (c) semua maklumat rahsia rasmi atas talian perlu berada dalam bentuk teks sifer sepanjang masa, manakala maklumat rahsia rasmi yang tidak diperlukan atas talian mesti dipindahkan segera ke media storan elektronik sekunder dalam bentuk teks sifer dan hendaklah dikelaskan.
- (d) maklumat penerimaan sesuatu dokumen rahsia rasmi hendaklah dilaksanakan melalui penggunaan dokumen akuan terima (Borang

Jadual) sepertimana di **Lampiran B**. 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.

6.6 Pelepasan Rahsia Rasmi

- (a) rahsia rasmi sama sekali tidak boleh disampaikan ke negara lain tanpa kebenaran Universiti dan 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 Universiti yang 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 satu garis panduan khusus berkaitan 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.

6.7 Pelupusan/ Pemusnahan

6.7.1 Peralatan yang mengandungi rahsia rasmi hendaklah dimusnahkan mengikut peraturan yang ditetapkan oleh Kerajaan dan dilakukan di bawah penyeliaan Pegawai Universiti yang dibenarkan untuk mengendalikan rahsia rasmi tersebut. Semua pemusnahan rahsia rasmi dan peralatannya hendaklah direkodkan.

6.7.2 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 perlu melalui sanitasi data mengikut peringkat yang ditetapkan seperti berikut:

Kaedah Sanitasi Data (Rahsia Besar/ Rahsia)

- (a) 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;
 - (i) tulis ganti secara fizikal;
 - (ii) penyingkiran (*purging*); dan
 - (iii) melaksanakan pemusnahan secara fizikal [perkara Rahsia Besar dan Rahsia] (*destroying*).
- (b) semua media yang berupaya menyimpan data adalah hak milik Universiti sepenuhnya dan sebarang pemulangan kepada pihak pembekal akibat daripada kerosakan kekal atau perlu ditukar ganti adalah tidak dibenarkan.
- (c) membuat validasi keselamatan di mana rekod validasi berkenaan pemusnahan rahsia rasmi hendaklah disahkan oleh pihak yang dibenarkan (*authorized entity*).

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.

6.8 Dasar Kriptografi Universiti

Penggunaan Produk Kriptografi Terpercaya adalah mandatori dalam urusan yang melibatkan rahsia rasmi. Sebarang penggunaan *Data Encryption Solution* hendaklah mendapat kelulusan Jawatankuasa Dasar Kriptografi Universiti .

7. PENGELASAN SEMULA RAHSIA RASMI

7.1 Prosedur pengelasan semula dokumen terperingkat boleh dibahagikan kepada tiga (3) peringkat seperti berikut:

- (a) Peringkat Pertama: Pra Pengelasan Semula
- (b) Peringkat Kedua: Semasa Pengelasan Semula
- (c) Peringkat Ketiga: Selepas Pengelasan Semula

7.2 Apa-apa suratan yang dinyatakan Dalam Jadual atau apa-apa suratan yang di Luar Jadual yang telah dikelaskan akan terhenti menjadi rahsia rasmi selepas pengelasan semula mengikut peruntukan Seksyen 2C Akta Rahsia Rasmi 1972 [Akta 88].

7.3 Naib Canselor mempunyai kuasa untuk mengelaskan semula dokumen rahsia rasmi Universiti.

7.4 Sebelum pengelasan semula dibuat dokumen rahsia rasmi disemak bagi menentukan:

- (a) bahawa surat berkaitan dimulakan (*originated*) oleh PTj tersebut sahaja;
- (b) bahawa surat berkaitan ialah surat rahsia rasmi sama ada Dalam Jadual ataupun di Luar Jadual; dan
- (c) bahawa kandungan surat berkaitan tidak lagi menyebabkan:
 - (i) kerosakan yang amat besar kepada Universiti atau kerajaan;
 - (ii) membahayakan keselamatan Universiti atau kerajaan; atau
 - (iii) keadaan serba-salah kepada Universiti atau kerajaan.

7.5 Selepas pengelasan semula dibuat, surat, maklumat atau bahan tersebut akan terhenti menjadi rahsia rasmi. Tatacara yang mesti dipatuhi dalam pengelasan semula rahsia rasmi dan diringkaskan sepertimana carta alir pada **Rajah 1**.

7.5.1 Pra Pengelasan Semula

- (a) Langkah Pertama - Kuasa Mengelaskan Semula
 - (i) dokumen rahsia rasmi hendaklah dikelaskan semula sebagaimana di peruntukan di bawah Seksyen 2C Akta Rahsia Rasmi 1972 [Akta 88] oleh Naib Canselor;
 - (ii) Naib Canselor boleh pada bila-bila masa mengelaskan semula mana-mana dokumen rahsia rasmi di dalam dan luar jadual;
 - (iii) tindakan pengelasan semula surat, bahan dan maklumat rahsia rasmi hendaklah ditentusahkan melalui tandatangan Naib Canselor dan beliau tidak boleh mewakili kuasanya bagi melaksanakan tugas tersebut kepada pegawai bawahannya kecuali sekiranya penurunan kuasa diberi kepada mana-mana Pegawai Universiti yang lain oleh Menteri Pengajian Tinggi di bawah peruntukan seksyen 5, Akta Perwakilan Kuasa 1956.

(b) Langkah Kedua – Suratan, Bahan atau Maklumat

Dokumen, maklumat atau bahan yang hendak dikelaskan semula mesti merupakan milik pemula di Universiti.

7.5.2 Semasa Pengelasan Semula

(a) Langkah Pertama - Jawatankuasa Menyemak

- (i) proses pengelasan semula yang hendak dilaksanakan perlulah mendapat kelulusan Jawatankuasa Menyemak yang terdiri daripada mereka yang mempunyai akses kepada dokumen rahsia rasmi.

Pengerusi : Pendaftar

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

(b) Langkah Kedua – Penilaian

- (i) penilaian melibatkan kandungan suratan rahsia rasmi supaya kandungannya tidak akan menyebabkan kerosakan yang amat besar kepada Universiti atau Kerajaan atau tidak membahayakan keselamatan Universiti atau Kerajaan ataupun tidak boleh menyebabkan Universiti atau Kerajaan dalam keadaan serba salah.
- (ii) Jawatankuasa Menyemak mengemukakan syor mereka kepada Pegawai Pengelas untuk membuat pengelasan semula rahsia rasmi tersebut, setelah penilaian yang dibuat tidak lagi mendatangkan kesan yang buruk kepada Universiti atau Kerajaan.

(c) Langkah Ketiga – Tempoh Rahsia Rasmi Disemak

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

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

Pengelasan semula dokumen rahsia rasmi hendaklah disenaraikan dengan menggunakan format borang pengelasan semula mengikut Seksyen 2C Akta Rahsia Rasmi 1972 [Akta 88] yang telah disediakan dan ditandatangani oleh Naib Canselor.

7.5.3 Selepas Pengelasan Semula

(a) Langkah Pertama – Cap '**TERBUKA**'

Cap Pengelasan Terbuka (Pengelasan Semula) Dokumen yang telah dikelaskan semula diberi penandaan cap 'Terbuka' tiap-tiap muka surat. Sekiranya dokumen tersebut kekal terjilid dan mempunyai muka surat yang tebal, dibolehkan untuk memberi cap 'Terbuka' pada lima (5) helaian pertama (termasuk muka/kulit hadapan), lima (5) muka surat pertengahan dan lima (5) muka surat terakhir (termasuk muka/kulit belakang).

(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;

Tindakan mendaftar ke dalam Buku Daftar Am 492 atau 492B yang mana berkenaan hendaklah dilaksanakan dan ditandatangani oleh Naib Canselor.

(c) Langkah Ketiga – Tanggungjawab Ketua Jabatan;

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.

8. PERUBAHAN PERINGKAT KESELAMATAN RAHSIA RASMI

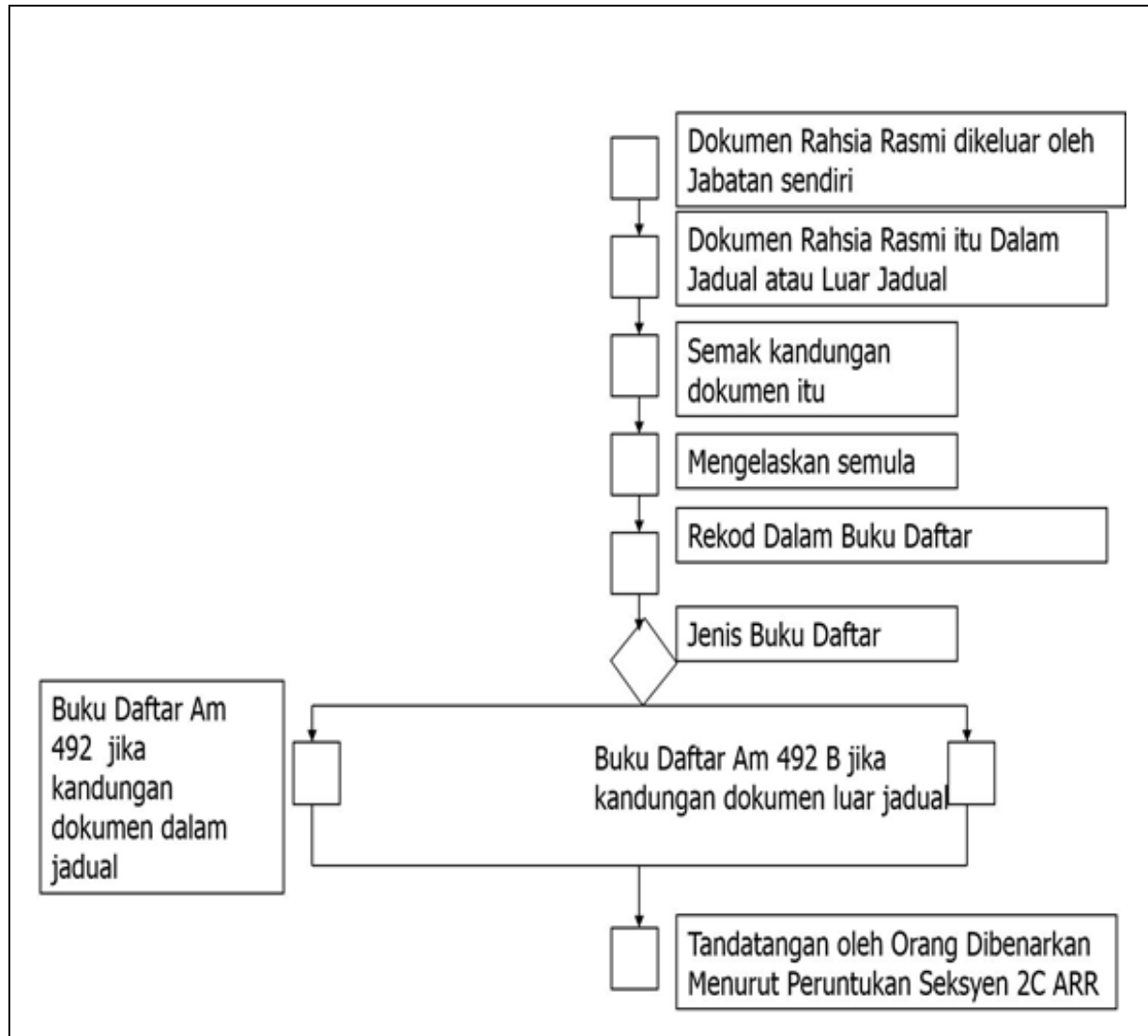
- 8.1 Jika terdapat keperluan untuk mengubah peringkat keselamatan sedia ada sesuatu rahsia rasmi sama ada ke peringkat yang lebih tinggi atau lebih rendah, pemula hendaklah memaklumkan kepada pihak yang memiliki rahsia rasmi akan perubahan peringkat keselamatan tersebut.
- 8.2 Bagi proses menaik taraf dokumen rahsia rasmi , Pegawai Universiti hendaklah memohon kepada Pegawai Pengelas melalui 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 Suratan Rahsia Rasmi.

9. TANGGUNGJAWAB

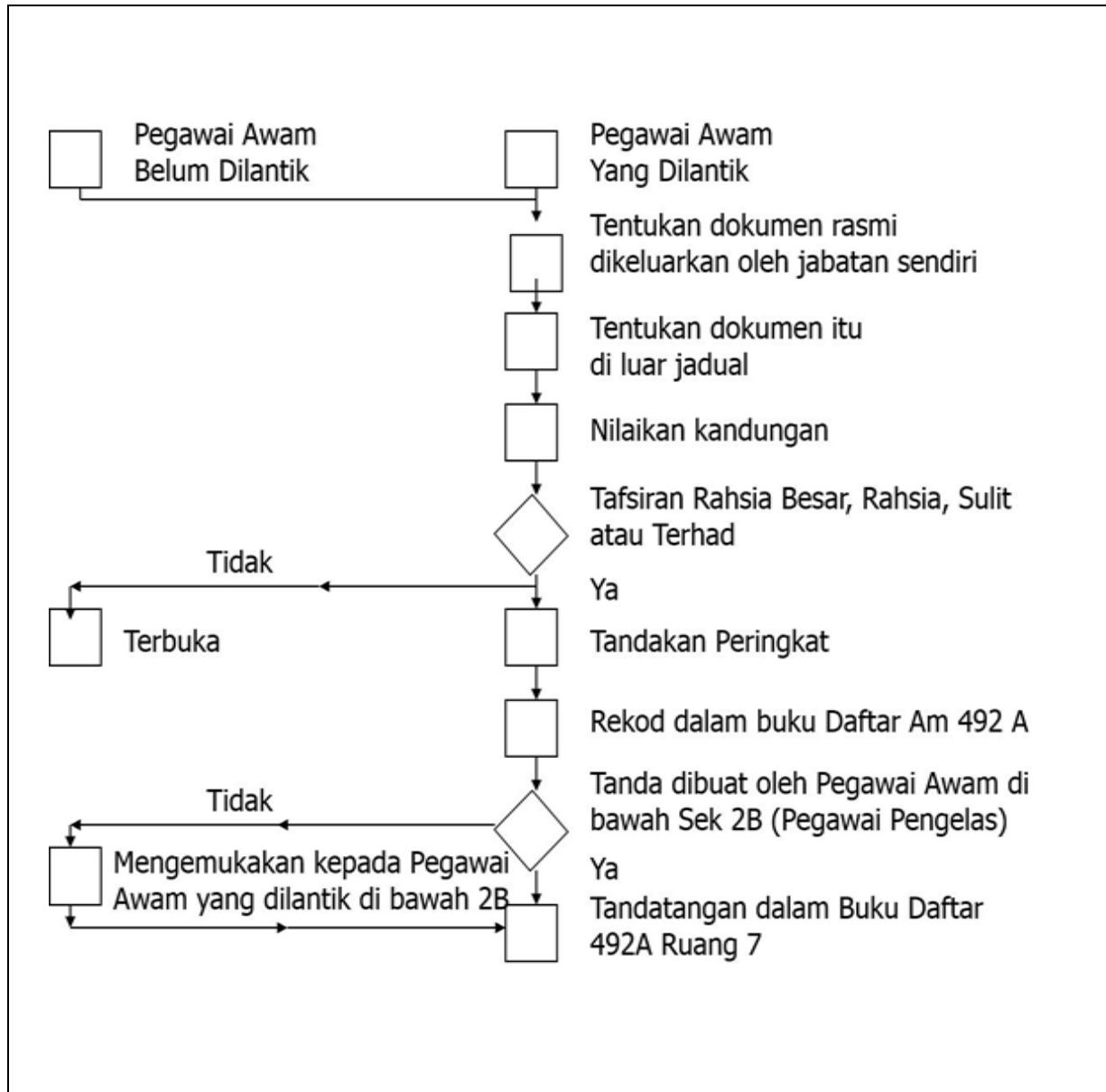
- 9.1 Jawatankuasa Pengurusan Universiti bertanggungjawab untuk:
- (a) meluluskan apa-apa perkara berhubungan dengan pengurusan Rahsia rasmi Universiti;
 - (b) menamakan Pegawai Pengelas untuk dilantik oleh Menteri;
 - (c) menubuhkan apa-apa jawatankuasa berkaitan pelaksanaan pengurusan rahsia rasmi Universiti; dan
 - (d) memastikan pematuhan pengurusan rahsia rasmi Universiti.
- 9.2 Pendaftar bertanggungjawab untuk:

- (a) mengesyorkan pelantikan Pegawai Universiti yang layak untuk mengelaskan dokumen rasmi;
- (b) melaksanakan pendaftaran dokumen rasmi yang dikelaskan dan dikelaskan semula dalam Buku Daftar Rahsia Rasmi Am 492 (di dalam Jadual dan Berhubung Dengannya), Buku Daftar Rahsia Rasmi Am 492A (di Luar Jadual dan Berhubung Dengannya yang dikelaskan) dan Buku Daftar Rahsia Rasmi Am 492B (di Luar Jadual dan Berhubung Dengannya yang dikelaskan semula) mengikut yang mana berkenaan. Carta Alir Luar Jadual adalah seperti di **Rajah 2**;
- (c) 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 sekiranya berlaku insiden kebocoran/ketirisan maklumat Universiti dan pendakwaan dijalankan di bawah Akta Rahsia Rasmi 1972 [Akta 88];
- (d) memaklumkan semua pihak terlibat mengikut suratan asal tersebut untuk memaklumkan bahawa suratan tersebut telah dikelaskan semula dan terhenti menjadi rahsia rasmi;
- (e) menghubungi Jabatan Arkib Negara Malaysia dan Pejabat Ketua Pegawai Keselamatan Kerajaan bagi mengkaji urusan pengelasan semula atau penurunan taraf peringkat atau pelupusan sewajarnya;
- (f) membangunkan dan menyemak garis panduan pengelasan dokumen rahsia rasmi dari semasa ke semasa;
- (g) menjalankan aktiviti inspektorat bagi memastikan garis panduan yang berkuat kuasa dipatuhi.

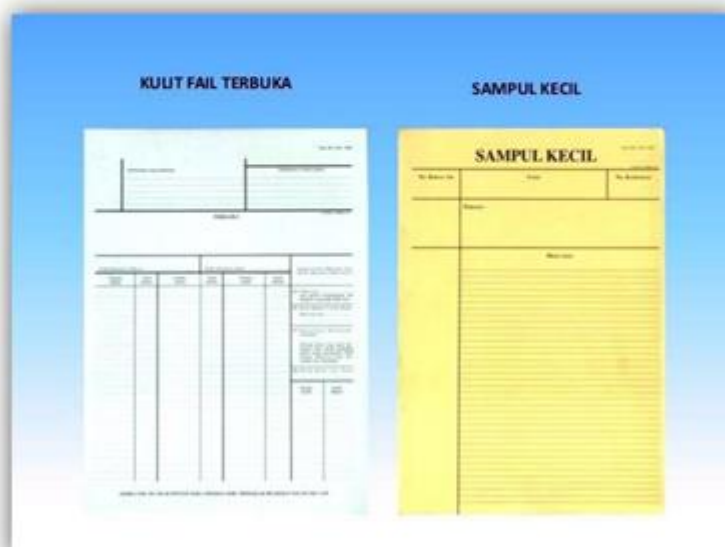
Rajah 1: Carta Alir Pengelasan Semula



Rajah 2: Carta Alir Pengelasan Rahsia Rasmi Luar Jadual



Lampiran A



No. Siri			
BORANG JADUAL PENGHANTARAN DOKUMEN RASMI			
Daripada :			
Kepada :		Tarikh :	
BIL.	TARIKH SURAT	BIL. RUJUKAN	PERKARA
.....POTONG DAN DIKEMBALIKAN AKUAN PENERIMAAN Kepada : No. Siri : Jadual telah disemak dan didapati betul. Tandatangan..... Cap Rasmi Jabatan : Tarikh..... Nama..... Jawatan.....			

Lampiran C

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 D

								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:	Nama Kementerian/Jabatan/Agensi yang membuat	
	Contoh:		
	Nama Kem/Jab/Agensi:	Pej. Ketua Pegawai Keselamatan Kerajaan Malaysia	
	Nama Kem/Jab/Agensi:	Jabatan Perdana Menteri	
(2)	Bahagian/Cawangan/Unit:	Bahagian/cawangan/unit yang terdapat dalam sesuatu Kementerian/Jabatan/Agensi yang membuat klasifikasi	
	Contoh:		
	Nama Bhg/Caw/Unit:	Bahagian Khidmat Pengurusan	
	Nama Bhg/Caw/Unit:	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		
(16)	Ruangan ini hendaklah diisi oleh Pegawai Pengelas yang dilantik di bawah Seksyen 2B, Akta Rahsia Rasmi 1972		