



BIRO PENGADUAN AWAM

PANDUAN PENGURUSAN KESELAMATAN DOKUMEN TERPERINGKAT

Bahagian Khidmat Pengurusan
Biro Pengaduan Awam
Jabatan Perdana Menteri
2014

TUJUAN

1. Panduan ini bertujuan untuk membantu warga Biro Pengaduan Awam (BPA) untuk mengurus keselamatan fizikal, dokumen, peribadi dan ICT di BPA.

LATAR BELAKANG

2. Panduan ini adalah disediakan berdasarkan Arahan Keselamatan, pekeliling dan arahan Kerajaan berkaitan pengurusan keselamatan perlindungan yang diguna pakai oleh Kementerian/Jabatan/Agensi Kerajaan.

3. Warga BPA selaku penjawat awam telah dipertanggungjawabkan untuk mengurus dokumen terperingkat kerajaan dikehendaki mematuhi sepenuhnya Arahan Keselamatan Kerajaan. Pematuhan kepada Arahan Keselamatan oleh warga BPA secara berterusan adalah perlu supaya maklumat dan dokumen rasmi Kerajaan dapat diberi perlindungan keselamatan sewajarnya.

4. Selaras dengan Arahan Keselamatan tersebut, hanya warga BPA yang telah menandatangani borang akuan berkenaan dengan Akta Rahsia Rasmi 1972 (Akta 88) dan lulus tapisan keselamatan sahaja yang dibenarkan mengurus dokumen terperingkat.

TAKRIF DAN KATEGORI DOKUMEN TERPERINGKAT

5. **Dokumen Terperingkat** merupakan dokumen atau surat rasmi yang mengandungi maklumat rasmi yang mesti diberi perlindungan untuk kepentingan keselamatan dan yang bertanda dengan sesuatu peringkat keselamatan. Maklumat dalam dokumen terperingkat mesti diberi perlindungan keselamatan berdasarkan Arahan Keselamatan dan peraturan berkaitan. Ia bertujuan untuk mengawal rahsia-rahsia BPA, Jabatan Perdana Menteri dan negara dengan berkesan. Di BPA, urusan pengendalian dan

penyimpanan dokumen terperingkat adalah perkara yang perlu diberi perhatian oleh semua warga BPA. Penjelasan atau keterangan mengenai Dokumen Terperingkat mengikut kategorinya adalah seperti berikut;

- i. **RAHSIA BESAR** - dokumen rasmi, maklumat rasmi dan bahan-bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada negara;
- ii. **RAHSIA** - dokumen rasmi, maklumat rasmi dan bahan rasmi jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing;
- iii. **SULIT** - dokumen rasmi, maklumat rasmi atau bahan rasmi jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia; dan
- iv. **TERHAD** - dokumen rasmi/maklumat rasmi/bahan rasmi selain daripada yang diperingkatkan **RAHSIA BESAR**, **RAHSIA** dan **SULIT** tetapi perlu diberi tahap perlindungan keselamatan.

PROSEDUR MENGURUS DOKUMEN TERPERINGKAT

6. Dalam memastikan keselamatan dan tahap kerahsiaan dokumen terperingkat di premis BPA sentiasa terjaga dan selamat dari sebarang penyalahgunaan oleh pihak tidak bertanggungjawab, warga BPA perlu mematuhi Arahan Keselamatan, pekeliling dan arahan Kerajaan berkaitan. Ia meliputi;

- i. peringkat keselamatan dokumen terperingkat;
- ii. tanda keselamatan dokumen terperingkat;
- iii. prosedur penyimpanan dokumen terperingkat;
- iv. prosedur penghantaran dokumen terperingkat;
- v. prosedur membawa dokumen terperingkat keluar pejabat;
- vi. prosedur pemusnahan dokumen terperingkat;
- vii. prosedur kehilangan dokumen terperingkat; dan
- viii. pengurusan dokumen terperingkat secara *digital*;

PERINGKAT KESELAMATAN DOKUMEN TERPERINGKAT

7. Dokumen rasmi, maklumat rasmi dan bahan rasmi yang diperingkatkan **RAHSIA BESAR** antaranya meliputi :

- i. Kertas-Kertas Jemaah Menteri mengenai dasar utama Kerajaan berkaitan perkara-perkara politik dan ekonomi;
- ii. Maklumat-maklumat mengenai perancangan gerakan dan penempatan barisan peperangan angkatan tentera jika berlaku perang;
- iii. Surat-menyurat dengan Kerajaan negara asing mengenai aspek perdagangan dan pertahanan; dan
- iv. Maklumat lengkap berkenaan dengan pertubuhan-pertubuhan perisikan Malaysia dan kaedah-kaedahnya.

8. Bagi fail **RAHSIA BESAR** hanya Ketua Pengarah BPA sahaja dibenarkan untuk menggunakan fail berkenaan. Pegawai lain yang ingin menggunakannya hendaklah mendapatkan kebenaran bertulis dari Ketua Pengarah BPA.

9. Dokumen rasmi, maklumat rasmi dan bahan rasmi yang dipertingkatkan **RAHSIA** pula antaranya meliputi :

- i. Arahan-arahan untuk perwakilan-perwakilan Malaysia yang membuat perundingan dalam negara asing;
- ii. Maklumat-maklumat mengenai pemasangan-pemasangan tentera; dan
- iii. Maklumat-maklumat mengenai pertubuhan-pertubuhan subversif dan kegiatan-kegiatannya.

10. 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 Ketua Pengarah BPA.

11. Dokumen rasmi, maklumat rasmi dan bahan rasmi yang diperingkatkan **SULIT** pula antaranya meliputi :

- i. Laporan-laporan perisikan biasa;
- ii. Dokumen-dokumen dan panduan-panduan teknik untuk kegunaan latihan tentera atau polis; dan
- iii. Maklumat-maklumat yang mungkin membolehkan pendapatan faedah kewangan daripadanya jika didedahkan sebelum masa.

12. Dokumen rasmi, maklumat rasmi dan bahan rasmi yang diperingkatkan **TERHAD** antaranya meliputi :

- i. Buku-buku Jabatan bagi maksud arahan;
- ii. Perintah-perintah dan arahan-arahan biasa Jabatan; dan
- iii. Dokumen-dokumen mengenai bekalan barang-barang dan alat-alat kelengkapan biasa tentera dan polis.

13. Warga BPA yang mengurus dokumen berkaitan Mesyuarat Jemaah Menteri (MJM) sama ada dalam bentuk *hard copy* atau *digital* perlu pada

setiap masa mematuhi peraturan keselamatan yang ditetapkan oleh Urusetia MJM iaitu Bahagian Kabinet, Perlembagaan dan Perhubungan Antara Kerajaan, Jabatan Perdana Menteri(JPM).

TANDA KESELAMATAN DOKUMEN TERPERINGKAT

14. Peringkat keselamatan hendaklah ditanda kepada dokumen terperingkat 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.

15. 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.

16. Peringkat keselamatan hendaklah ditanda kepada dokumen terperingkat 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.

17. Peringkat keselamatan hendaklah ditanda kepada gambar, filem dan lukisan terperingkat supaya peringkatnya dapat dilihat pada salinan yang dibuat daripadanya. Sebagai tambahan peringkat keselamatan hendaklah ditanda di sebelah belakang gambar, filem dan lukisan berkenaan.

18. 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.

19. Hanya tajuk fail **TERHAD** sahaja boleh dicatatkan di sebelah luar kulit hadapan.

PROSEDUR PENYIMPANAN DOKUMEN TERPERINGKAT

20. Perkara-perkara terperingkat hendaklah disimpan dalam peti-peti keselamatan yang sewajarnya dengan peringkatnya seperti berikut:

- i. Dokumen terperingkat **RAHSIA BESAR** hendaklah disimpan dalam bilik kebal atau peti besi yang seelok-eloknya dipasang dengan kunci tatakira;
- ii. Dokumen terperingkat **RAHSIA** hendaklah disimpan dalam cabinet keluli atau almari keluli yang dipasang dengan palang besi berkunci; dan
- iii. Dokumen terperingkat **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.

21. Perkara terperingkat yang lain daripada dokumen terperingkat termasuk buangan terperingkat 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.

22. Perkara terperingkat yang ditinggalkan untuk jangka waktu yang singkat atau panjang hendaklah sentiasa dikunci bagi menghindari orang-orang tidak dibenarkan daripada dapat memperhatikan dan memperolehi perkara-perkara terperingkat.

PROSEDUR PENGHANTARAN DOKUMEN TERPERINGKAT

23. Penghantaran dokumen terperingkat dalam negeri hendaklah mematuhi prosedur berikut:

- i. Mendapatkan satu resit akuan terima (seperti yang dinyatakan dalam Borang Jadual Lampiran G, Arahan Keselamatan);
- ii. Menyemak Borang Jadual;
- iii. Memastikan resit diterima semula;
- iv. Dihantar melalui peti atau beg berkunci;
- v. Dihantar melalui sistem dua lapis sampul surat;
- vi. Dihantar melalui Utusan Selamat; dan
- vii. Dihantar melalui Akuan Terima Berdaftar.

24. Penghantaran dokumen keluar negara hendaklah diuruskan melalui Pendaftar Rahsia, Kementerian Luar Negeri.

PROSEDUR MEMBAWA DOKUMEN TERPERINGKAT KELUAR PEJABAT

25. Dokumen terperingkat **RAHSIA BESAR, RAHSIA, SULIT** atau **TERHAD** yang akan dibawa keluar dari premis BPA hendaklah mendapat kebenaran bertulis daripada Ketua Pengarah BPA.

PROSEDUR KEHILANGAN DOKUMEN TERPERINGKAT

26. Dokumen terperingkat yang hilang hendaklah dilaporkan dengan segera kepada Ketua Pengarah BPA atau Pegawai Keselamatan Jabatan yang akan menyiasat dan mengemukakan laporan kepada Pegawai Keselamatan Kerajaan dalam masa 24 jam.

27. Jika dokumen terperingkat tersebut terbukti hilang, Ketua Pengarah BPA hendaklah menimbang sama ada tindakan tatatertib diambil atau penyiasatan di bawah Akta Rahsia Rasmi 1972 (Akta 88) perlu dijalankan.

28. Laporan ke balai polis yang terdekat hendaklah dibuat sekiranya difikirkan sesuatu kesalahan jenayah telah berlaku.

PROSEDUR PEMUSNAHAN DOKUMEN TERPERINGKAT

29. Dokumen terperingkat 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'**.

30. Apabila dokumen **RAHSIA BESAR** dimusnahkan, satu sijil pemusnahan hendaklah dihantar kepada kuasa pemula dokumen tersebut.

31. Rujukan kepada Ketua Pegawai Keselamatan Kerajaan atau Ketua Pengarah Arkib Negara hendaklah dibuat terlebih dahulu oleh pihak BPA di atas segala cadangan pemusnahan dokumen terperingkat.

32. Dokumen terperingkat termasuk buangan terperingkat 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.

33. Buangan terperingkat hendaklah diberikan perlindungan keselamatan yang sepatutnya sehingga dimusnahkan.

34. Rujukan kepada Pegawai Keselamatan Kerajaan hendaklah dibuat bagi lain-lain cara pemusnahan.

PENGURUSAN DOKUMEN TERPERINGKAT SECARA *DIGITAL*

35. Kuasa pengurusan dan pengendalian dokumen terperingkat secara *digital* adalah sama seperti peringkat keselamatan dokumen terperingkat yang dinyatakan di atas iaitu hanya Ketua Pengarah BPA sahaja dibenarkan untuk mengendalikan semua dokumen terperingkat **RAHSIA BESAR** secara *digital*. Pegawai lain yang ingin mengendalikan fail RAHSIA BESAR perlulah mendapatkan kebenaran bertulis dari Ketua Pengarah BPA.

36. Hanya Pegawai Gred 54 dan ke atas sahaja dibenarkan mengendalikan fail berstatus **RAHSIA** secara *digital*. Pegawai Gred 52 dan ke bawah hendaklah mendapatkan kebenaran bertulis daripada Pengarah Bahagian berkenaan di BPA apabila ingin mengendalikan fail terperingkat tersebut secara *digital*.

37. Semua warga BPA yang berstatus perkhidmatan sementara tidak dibenarkan untuk mengendalikan dokumen terperingkat **RAHSIA BESAR** dan **RAHSIA** secara *digital*. Mereka ini hanya dibenarkan untuk mengendalikan dokumen-dokumen **SULIT** dan **TERHAD** secara *digital* hanya dalam keadaan terkecuali sahaja dengan kebenaran Ketua Pengarah BPA.

38. Warga BPA yang mengendalikan dokumen terperingkat secara *digital* hendaklah mematuhi peruntukan semua peraturan serta pekeliling dan panduan berkaitan keselamatan teknologi maklumat dalam mengendalikan dokumen terperingkat secara *digital*. Antara pekeliling berkaitan ialah :

- i. Pekeliling Am Bil. 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
- ii. Pekeliling Kemajuan Perkhidmatan Awam Bil. 1 Tahun 2003 – Panduan Mengenai Tatacara Penggunaan Internet dan Mel *Digital* di Agensi-Agensi Kerajaan;

- iii. Arahan Keselamatan;
- iv. Akta Rahsia Rasmi 1972 (Akta 88); dan
- v. Akta Arkib Negara 2003 (Akta 629).

39. Untuk keselamatan dokumen terperingkat yang disedia, disimpan dan diedar secara *digital*, ia perlu dienkrip untuk mengelakkan ia dibuka dan dibaca oleh pihak yang tidak bertanggungjawab.

40. Proses enkripsi dilakukan dengan menukarkan data atau maklumat tersebut ke dalam bentuk rahsia di mana hanya penerima yang sah sahaja dapat memahaminya dan hanya penerima yang sah itu sahaja yang boleh melakukan proses dekripsi, iaitu proses menterbalikkan kembali proses enkripsi supaya data atau maklumat ditukar ke bentuk yang asal.

KAWALAN KOMPUTER

41. Apabila pengguna diberi kebenaran untuk menggunakan sistem atau rangkaian, adalah perlu untuk menghadkan kebenaran tersebut ke tahap set yang paling minima bersamaan dengan keperluan melaksanakan tugas yang efektif. Pada kebiasaannya had akses minimum bermakna tidak boleh akses. Seterusnya akses untuk membaca atau melihat sahaja, mewujudkan, kemaskini, mengubah atau memadam boleh diberikan tetapi hendaklah berpandukan peruntukan dasar dan dengan kelulusan tertentu. Pelaksanaan akses kawalan adalah berbeza bergantung kepada sistem ICT tetapi pada amnya melibatkan kebenaran membaca, menulis dan memadam.

42. Semua pengguna sistem komputer akan disediakan dengan kod pencaman pengguna (User-Id) bagi membolehkannya membuat capaian.

- i. Setiap pengguna akan diberikan kod pencaman pengguna yang tidak boleh dikongsi; dan

- ii. Pengguna mestilah menyediakan pengesahan (authentication) (i.e kata laluan) yang hanya diketahui oleh pengguna berkenaan.

43. Kata laluan perlu dikawal untuk mengelakkan daripada diketahui oleh orang yang tidak diberi kuasa menggunakannya:

- i. Kata laluan tidak boleh dicatat di atas kertas;
- ii. Kata laluan mestilah mempunyai kombinasi sekurang-kurangnya enam askara;
- iii. Kata laluan perlu ditukar sekurang-kurangnya setiap enam bulan;
- iv. Kata laluan yang disimpan dalam komputer akan dikod (encrypted);
- v. Kata laluan dimasukkan pada medan tanpa boleh lihat; dan
- vi. Had percubaan dari segi masa atau bilangan percubaan akan ditetapkan untuk memasukkan kata laluan dan pencaman pengguna. Sekiranya kemasukan tidak berjaya dalam had tersebut, percubaan seterusnya tidak akan dibenarkan.

44. Untuk memastikan perkhidmatan komputer dan rangkaian yang disediakan tidak terganggu, semua sistem dilengkapi dengan perisian "virus-screening". Perisian ini hendaklah digunakan untuk mengimbas semua perisian pihak ketiga atau dari lain-lain agensi atau sumber; pengimbasan hendaklah dilakukan sebelum perisian dilaksanakan.

45. Untuk memastikan perkhidmatan komputer dan rangkaian yang disediakan tidak terganggu, semua sistem dilengkapi dengan perisian "virus-screening". Perisian ini hendaklah digunakan untuk mengimbas semua perisian pihak ketiga atau dari lain-lain agensi atau sumber; pengimbasan hendaklah dilakukan sebelum perisian dilaksanakan.

PEMAKAIAN

46. Panduan ini terpakai untuk semua premis BPA di Ibu Pejabat dan di Negeri.

TARIKH KUAT KUASA

47. Panduan ini berkuat kuasa **mulai 1 Januari 2013**.

**Bahagian Khidmat Pengurusan
Biro Pengaduan Awam
1 Januari 2014**

NOTA