



JABATAN AKAUNTAN NEGARA MALAYSIA

GARIS PANDUAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

VERSI 1.1

2024



**SEJARAH DOKUMEN
GARIS PANDUAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI**

TAHUN	NAMA DOKUMEN	VERSI	KELULUSAN	TARIKH KUATKUASA
2022	Garis Panduan Teknologi Maklumat Dan Komunikasi	1.0	JPICT JANM	6 Julai 2022
2024	Garis Panduan Teknologi Maklumat Dan Komunikasi	1.1	JPICT JANM	4 Julai 2024



**JADUAL PINDAAN
GARIS PANDUAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI**

TARIKH	VERSI	JENIS PINDAAN
6 Julai 2022	1.0	Semakan mengikut dokumen Polisi Keselamatan Siber versi 1.0.
4 Julai 2024	1.1	Semakan mengikut dokumen Polisi Keselamatan Siber versi 1.1 dan tambahan melibatkan perkara baharu berdasarkan ISO/IEC27001:2022



ISI KANDUNGAN

PERKARA	MUKASURAT
1.0 TUJUAN	4
2.0 SKOP	4
3.0 PENGGUNA	5
4.0 RUJUKAN.....	5
5.0 AKAUN DAN CAPAIAN MAKLUMAT	7
6.0 E-MEL RASMI	10
7.0 RANGKAIAN ICT	15
8.0 PERKAKASAN DAN PERISIAN	19
9.0 PENGURUSAN KESELAMATAN SISTEM APLIKASI	21
10.0 PERKHIDMATAN PRASARANA KUNCI AWAM – <i>GOVERNMENT PUBLIC KEY INFRASTRUCTURE (GPKI)</i>	26
11.0 PIHAK KETIGA	28
12.0 GLOSARI.....	30
LAMPIRAN 1 : Borang Permohonan <i>Virtual Private Network (VPN)</i> Jabatan Akauntan Negara	
LAMPIRAN 2 : Borang Permohonan Penamatan <i>Virtual Private Network (VPN)</i> Jabatan Akauntan Negara	
LAMPIRAN 3 : Borang Perakuan Untuk Ditandatangani Oleh Komuniti Keselamatan Atau Mana-Mana Pihak Lain yang Berurusan Dengan Perkhidmatan Awam Atau Yang Berkhidmat di Kediaman Rasmi Kerajaan Berkaitan Dengan Akta Rahsia Rasmi 1972 [Akta 88]	
LAMPIRAN 4 : Borang Perakuan Untuk Ditandatangani oleh Komuniti Keselamatan Atau Mana-Mana Pihak Lain yang Berurusan Dengan Perkhidmatan Awam atau Yang Berkhidmat di Kediaman Rasmi Kerajaan Apabila Tamat Kontrak Perkhidmatan Dengan Kerajaan Berkaitan dengan Akta Rahsia Rasmi 1972 [Akta 88]	



1.0 TUJUAN

Garis Panduan Teknologi Maklumat dan Komunikasi Jabatan Akauntan Negara Malaysia (JANM) merupakan dokumen sokongan yang perlu dibaca bersama dengan Polisi Keselamatan Siber JANM versi 1.1 Tahun 2024.

2.0 SKOP

Garis Panduan Teknologi Maklumat ini menerangkan tatacara penggunaan dan pengendalian kawalan Keselamatan yang meliputi perkara berikut:

- a. Akaun dan Capaian;
- b. E-mel Rasmi;
- c. Rangkaian dan Keselamatan;
- d. Perkakasan dan Perisian;
- e. Perkhidmatan Prasarana Kunci Awam – *Government Public Key Infrastructure* (GPKI);
- f. Pengurusan Keselamatan Sistem Aplikasi; dan
- g. Pihak Ketiga.



3.0 PENGGUNA

Pengguna meliputi:

Pengguna	Keterangan
Warga JANM	Personel kerajaan yang berkhidmat di JANM sama ada berjawatan tetap, sambilan dan kontrak yang menggunakan perkhidmatan ICT JANM.
Pihak Ketiga	Pembekal, perunding dan pihak yang berurusan dengan pihak JANM serta pengguna sistem JANM yang lain (bertujuan untuk akses data JANM).

4.0 RUJUKAN

- a. Polisi Keselamatan Siber JANM versi terkini; dan
- b. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) versi terkini.



AKAUN DAN CAPAIAN MAKLUMAT



5.0 AKAUN DAN CAPAIAN MAKLUMAT

Bil.	Perkara	Peranan
1.	<p>a. Penggunaan kata laluan pada setiap perkakasan ICT (<i>server</i> dan komputer) adalah diwajibkan.</p> <p>b. Penentuan kata laluan mesti mematuhi perkara berikut:-</p> <ul style="list-style-type: none">• Tetapan kata laluan perlu memenuhi kerumitan (<i>complexity</i>);• Mempunyai huruf besar, huruf kecil, nombor dan simbol. Contohnya P@\$\$w0rd1234;• Panjang kata laluan mesti sekurang-kurangnya dua belas (12) aksara KECUALI bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad;• Penguatkuasaan pertukaran kata laluan semasa atau selepas <i>login</i> kali pertama atau selepas reset kata laluan;• Kata laluan yang sama boleh digunakan semula selepas tiga (3) kali pusingan;• Kata laluan menyerupai <i>username</i> tidak dibenarkan;• Kata laluan mesti ditukar dalam tempoh maksima enam (6) bulan atau 180 hari;• Pengguna mesti menukar kata laluan dalam kadar segera apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; dan• Menyimpan kata laluan menggunakan fungsi <i>autosave</i> di pelayar (<i>browser</i>) adalah tidak dibenarkan. <p>c. Kata laluan tidak boleh ditulis, dipamer dan diletakkan pada komputer atau kawasan kerja.</p>	<ul style="list-style-type: none">• Warga JANM• Pihak ketiga



Bil.	Perkara	Peranan
2	<p>a. Penamatan semua capaian bagi sistem, perkakasan dan perisian perlu dilaksanakan untuk warga JANM melibatkan kategori berikut:</p> <ul style="list-style-type: none">• Tamat perkhidmatan,• Berpindah atau bertukar jabatan,• Berkursus bagi tempoh melebihi enam (6) bulan, dan;• Bercuti bagi tempoh tiga (3) bulan dan ke atas,	<ul style="list-style-type: none">• Warga JANM
3.	<p>a. Memastikan kawalan terhadap perkakasan, perisian dan fasiliti pusat data daripada capaian yang tidak dibenarkan, kecurian dan kemusnahan.</p> <p>b. Komputer mesti ditutup (<i>log off</i>) sepenuhnya pada akhir hari kerja.</p> <p>c. Memastikan semua maklumat sensitif atau sulit dalam bentuk salinan atau elektronik adalah selamat apabila hendak meninggalkan kawasan kerja.</p> <p>d. Dokumen Terhad atau Sulit yang tidak lagi diperlukan hendaklah dihapuskan secara dirincih; merujuk kepada Arkib Negara.</p>	<ul style="list-style-type: none">• Warga JANM• Pihak ketiga
4.	<p>a. <i>Content Filtering</i></p> <p>Perisian <i>Content Filtering</i> mestilah digunakan bagi mengawal akses internet mengikut fungsi kerja dan pemantauan tahap pematuhan. Kawalan akses internet berdasarkan Garis Panduan Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan yang berkuatkuasa.</p>	<ul style="list-style-type: none">• Warga JANM• Pihak ketiga



E-MEL RASMI



6.0 E-MEL RASMI

Bil.	Perkara	Peranan									
1.	<p><u>Permohonan E-mel Rasmi</u></p> <p>a. Permohonan perkhidmatan e-mel rasmi bagi pegawai baharu di JANM dilaksanakan melalui dua (2) kaedah mengikut kategori pengguna seperti berikut:</p> <table border="1"><thead><tr><th>Bil</th><th>Kategori pengguna</th><th>Kaedah permohonan</th></tr></thead><tbody><tr><td>1.</td><td>Pengurusan Tertinggi (Akauntan Negara Malaysia/ Timbalan Akauntan Negara (Operasi)/ Timbalan Akauntan Negara (Korporat)/ Pegarah Bahagian/ Pegarah JANM Negeri dan Cawangan/ Timbalan Pegarah Bahagian/ Pegarah JANM Negeri dan Cawangan)</td><td>Permohonan perkhidmatan e-mel rasmi bagi pegawai baharu di JANM memerlukan pengisian Borang Permohonan Perkhidmatan MyGovUC Dan <i>Active Directory</i> JANM bagi mewujudkan akaun pegawai baharu di JANM oleh Pentadbir UC. Lampiran 1: Borang Permohonan Perkhidmatan MyGovUC Dan <i>Active Directory</i> JANM</td></tr><tr><td>2.</td><td>Warga JANM</td><td>Permohonan ini memerlukan pengisian Borang Permohonan Perkhidmatan MyGovUC Dan <i>Active Directory</i> JANM melalui Sistem iManage. (https://imange.anm.gov.my) Pengesahan Ketua Unit/ Seksyen/ Bahagian masing-masing diperlukan bagi mewujudkan akaun pegawai baharu di JANM oleh Pentadbir UC.</td></tr></tbody></table>	Bil	Kategori pengguna	Kaedah permohonan	1.	Pengurusan Tertinggi (Akauntan Negara Malaysia/ Timbalan Akauntan Negara (Operasi)/ Timbalan Akauntan Negara (Korporat)/ Pegarah Bahagian/ Pegarah JANM Negeri dan Cawangan/ Timbalan Pegarah Bahagian/ Pegarah JANM Negeri dan Cawangan)	Permohonan perkhidmatan e-mel rasmi bagi pegawai baharu di JANM memerlukan pengisian Borang Permohonan Perkhidmatan MyGovUC Dan <i>Active Directory</i> JANM bagi mewujudkan akaun pegawai baharu di JANM oleh Pentadbir UC. Lampiran 1: Borang Permohonan Perkhidmatan MyGovUC Dan <i>Active Directory</i> JANM	2.	Warga JANM	Permohonan ini memerlukan pengisian Borang Permohonan Perkhidmatan MyGovUC Dan <i>Active Directory</i> JANM melalui Sistem iManage. (https://imange.anm.gov.my) Pengesahan Ketua Unit/ Seksyen/ Bahagian masing-masing diperlukan bagi mewujudkan akaun pegawai baharu di JANM oleh Pentadbir UC.	<ul style="list-style-type: none">Warga JANM
Bil	Kategori pengguna	Kaedah permohonan									
1.	Pengurusan Tertinggi (Akauntan Negara Malaysia/ Timbalan Akauntan Negara (Operasi)/ Timbalan Akauntan Negara (Korporat)/ Pegarah Bahagian/ Pegarah JANM Negeri dan Cawangan/ Timbalan Pegarah Bahagian/ Pegarah JANM Negeri dan Cawangan)	Permohonan perkhidmatan e-mel rasmi bagi pegawai baharu di JANM memerlukan pengisian Borang Permohonan Perkhidmatan MyGovUC Dan <i>Active Directory</i> JANM bagi mewujudkan akaun pegawai baharu di JANM oleh Pentadbir UC. Lampiran 1: Borang Permohonan Perkhidmatan MyGovUC Dan <i>Active Directory</i> JANM									
2.	Warga JANM	Permohonan ini memerlukan pengisian Borang Permohonan Perkhidmatan MyGovUC Dan <i>Active Directory</i> JANM melalui Sistem iManage. (https://imange.anm.gov.my) Pengesahan Ketua Unit/ Seksyen/ Bahagian masing-masing diperlukan bagi mewujudkan akaun pegawai baharu di JANM oleh Pentadbir UC.									



**GARIS PANDUAN TEKNOLOGI MAKLUMAT
DAN KOMUNIKASI**

Versi : 1.1

Tahun : 2024

Bil.	Perkara	Peranan
	<p>b. Pengguna baharu perlu menukar kata laluan sementara, apabila diberikan pada login kali pertama.</p> <p>c. Rahsiakan dan kukuhkan kata laluan e-mel. Penentuan kata laluan mestilah mematuhi kerumitan (<i>complexity</i>) yang telah ditetapkan.</p> <p>d. Saiz storan untuk semua pengguna adalah tertakluk kepada polisi dan ketetapan daripada pihak penyedia perkhidmatan MyGovUC iaitu Jabatan Digital Negara (JDN).</p> <p>e. Pengguna perlu menukar kata laluan apabila disyaki berlakunya kebocoran atau dikompromi. Kata laluan hendaklah diingat dan TIDAK BOLEH didedahkan dengan apa cara sekalipun.</p> <p>f. Pemohonan akaun e-mel akan diproses dalam tempoh lima (5) hari bekerja.</p>	



2.	<p><u>Penggunaan E-mel</u></p> <p>a. Memastikan penghantaran e-mel rasmi menggunakan akaun e-mel rasmi JANM @anm.gov.my dan alamat penerima yang betul.</p> <p>b. Perkhidmatan e-mel menyediakan penghantaran fail kepilan berdasarkan penetapan saiz kepilan (<i>attachment</i>) adalah seperti penetapan dibawah:</p> <table border="1" data-bbox="320 595 1201 786"><thead><tr><th>Bil.</th><th>Saiz Kepilan</th><th>Kaedah Penghantaran Kepilan</th></tr></thead><tbody><tr><td>1.</td><td><10MB</td><td>E-mel</td></tr><tr><td>2.</td><td>>10MB</td><td>Storan <i>cloud</i></td></tr></tbody></table> <p>c. Setiap pengguna bertanggungjawab untuk menguruskan e-mel masing-masing bagi memastikan e-mel yang disimpan tidak melebihi saiz <i>mailbox</i> yang telah diperuntukkan. Sekiranya kapasiti telah digunakan sepenuhnya, e-mel yang baru tidak akan diterima oleh sistem.</p> <p>d. Pengguna bertanggungjawab sepenuhnya terhadap semua kandungan e-mel dan lampiran fail.</p> <p>e. Akaun e-mel yang tidak aktif untuk tempoh 90 hari akan ditamatkan kecuali perlanjutan tempoh telah dimaklumkan kepada Pentadbir e-mel.</p>	Bil.	Saiz Kepilan	Kaedah Penghantaran Kepilan	1.	<10MB	E-mel	2.	>10MB	Storan <i>cloud</i>	<ul style="list-style-type: none">Warga JANM
Bil.	Saiz Kepilan	Kaedah Penghantaran Kepilan									
1.	<10MB	E-mel									
2.	>10MB	Storan <i>cloud</i>									
3.	<p><u>Keselamatan E-mel</u></p> <p>a. Memastikan fungsi enkripsi digunakan untuk menghantar e-mel yang mengandungi maklumat Rahsia Rasmi (Rahsia Besar, Rahsia, Sulit dan Terhad) melalui sistem e-mel Kerajaan.</p> <p>b. Kegiatan e-mel pengguna akan dipantau untuk tujuan penguatkuasaan dan dijadikan bahan bukti untuk kes rasmi di mahkamah.</p> <p>c. Memastikan setiap fail yang dimuat naik dan muat turun bebas daripada virus sebelum digunakan.</p> <p>d. Pengguna digalakkan membuat salinan/ arkib e-mel secara berasingan bagi tujuan <i>backup</i>.</p> <p>e. Membuat aduan atau laporan rasmi kepada Pentadbir e-mel jika menerima kandungan e-mel yang disertakan dengan bahan yang terlarang.</p>	<ul style="list-style-type: none">Warga JANM									



	f. Memaklumkan kepada pentadbir e-mel dengan segera sekiranya mengesyaki akaun telah disalahgunakan.	
4.	<p><u>Penamatan atau Nyahaktif E-mel</u></p> <p>a. Pegawai bertanggungjawab di setiap Bahagian dan JANM Negeri/ Cawangan perlu memaklumkan kepada Pentadbir e-mel tiga (3) hari bekerja selepas mana-mana warga JANM yang tamat perkhidmatan atau bertukar Jabatan atau cuti belajar atau kursus melebihi enam (6) bulan atau cuti melebihi tiga (3) bulan.</p> <p>b. Akaun e-mel bagi warga JANM yang cuti belajar atau cuti melebihi tiga (3) bulan perlu dinyahaktif (<i>disable</i>) dalam tempoh tiga (3) hari bekerja.</p> <p>c. Akaun e-mel perlu ditamatkan 30 hari dari tarikh pengguna tamat perkhidmatan di JANM.</p>	<ul style="list-style-type: none">• Warga JANM
5.	<p>Perkara-perkara berikut adalah <u>TIDAK DIBENARKAN</u>:</p> <p>a. Penggunaan e-mel selain daripada e-mel rasmi Kerajaan bagi urusan rasmi.</p> <p>b. Kemudahan e-mel untuk menghantar bahan-bahan yang salah di sisi undang-undang seperti bahan lucah, perjudian, jenayah, cetak rompak atau apa-apa maklumat yang menjejaskan reputasi JANM.</p> <p>c. Kemudahan e-mel rasmi untuk tujuan peribadi, komersial atau politik.</p> <p>d. Menyimpan, memuat turun dan memuat naik bahan yang mempunyai hakcipta, termasuk yang dimuat turun dari Internet atau menyebarkan kepada pihak lain tanpa mendapat kebenaran terlebih dahulu daripada pemilik hak cipta yang berkenaan.</p> <p>e. Menghantar e-mel sampah (<i>junk mail</i>) dan e-mel <i>spam</i> serta menyebarkan kod perosak seperti <i>virus</i>, <i>worm</i>, dan <i>trojan horse</i> yang boleh merosakkan sistem komputer dan maklumat pengguna lain.</p> <p>f. Menggunakan akaun milik orang lain, berkongsi akaun atau memberi akses akaun kepada orang lain untuk menjawab e-mel bagi pihaknya.</p>	<ul style="list-style-type: none">• Warga JANM



RANGKAIAN ICT



7.0 RANGKAIAN ICT

Bil.	Perkara	Peranan
1.	<p><u>Rangkaian</u></p> <p>Memastikan semua peranti infrastruktur Rangkaian yang disambungkan ke rangkaian JANM</p> <ul style="list-style-type: none">• Mematuhi piawaian yang ditetapkan dalam Standard Komunikasi;• Menggunakan protokol dan infrastruktur pengesahan yang diluluskan;• Menggunakan protokol penyulitan JANM yang diluluskan; dan• Peranti berupaya menyimpan alamat MAC perkakasan yang menggunakan rangkaian.	<ul style="list-style-type: none">• Warga JANM• Pihak ketiga
2.	<p><u>Rangkaian Tanpa Wayar (<i>Wireless</i>)</u></p> <p>Menggunakan <i>Service Set Identifier</i> (SSID) rangkaian tanpa wayar berdasarkan peranan pengguna seperti berikut:</p> <ul style="list-style-type: none">• Pelawat JANM (JANM-GUEST-HQ);• Pengguna dalaman (JANM-STAFF-HQ);• Pengguna Teknikal (JANM-TECH-HQ);• Pembekal (JANM-VENDOR-HQ); dan• SSID Negeri dan cawangan.	<ul style="list-style-type: none">• Warga JANM• Pihak ketiga
3.	<p><u>Virtual Private Network (VPN)</u></p> <p>a. Semua capaian rasmi kepada sistem JANM secara jarak jauh hendaklah menggunakan perkhidmatan VPN yang disediakan oleh pihak BPTM.</p> <p>b. VPN adalah sambungan rangkaian yang dilindungi ketika menggunakan rangkaian awam. VPN menyulitkan (<i>encrypt</i>) lalu lintas internet anda dan menyamarkan identiti dalam talian anda. Ini menyukarkan pihak luar untuk mengesan aktiviti anda dalam talian dan mencuri data. Penyulitan berlaku dalam masa nyata.</p> <p>c. Pengguna VPN perlu mematuhi peraturan berikut:</p> <ul style="list-style-type: none">• Menggunakan komputer hak milik kerajaan SAHAJA yang dilengkapi dengan kata laluan (<i>password</i>);• Memastikan perisian antivirus berlesen; atau perisian keselamatan	<ul style="list-style-type: none">• Warga JANM• Pihak ketiga



Bil.	Perkara	Peranan
	<p>enkripsi atau dekripsi;</p> <ul style="list-style-type: none">• Status Polisi Keselamatan Siber JANM telah disahkan; dan• Pemohonan akaun VPN akan diproses dalam tempoh tiga (3) hari bekerja. <p>d. Borang Permohonan Pendaftaran VPN Jabatan Akauntan Negara Malaysia adalah seperti di Lampiran 1.</p> <p><u>Virtual Private Network (VPN)- bertempoh</u></p> <p>a. VPN (Bertempoh) Akses kepada rangkaian dalaman JANM diberikan kepada warga JANM dan pihak ketiga yang berdaftar ketika dalam situasi kritikal seperti bencana alam, pandemik dan sebagainya.</p> <p>b. Pengguna VPN perlu mematuhi peraturan berikut:</p> <ul style="list-style-type: none">• Menggunakan komputer hak milik kerajaan SAHAJA yang dilengkapi dengan Kata laluan (<i>password</i>);• Memastikan perisian antivirus berlesen; atau Perisian keselamatan enkripsi atau dekripsi;• Status Polisi Keselamatan Siber JANM telah disahkan;• Pemohonan akaun VPN akan diproses dalam tempoh tiga (3) hari bekerja; dan• Tidak mengakses VPN menggunakan rangkaian awam.	
4.	<p><u>Penamatan atau Nyahaktif Virtual Private Network (VPN)</u></p> <p>a. ID <i>Virtual Private Network</i> (VPN) bagi kakitangan akan dinyahaktifkan sekiranya tidak diakses selama enam (6) bulan berturut-turut dan ID akan dipadamkan pada bulan berikutnya.</p> <p>b. ID <i>Virtual Private Network</i> (VPN) bagi pihak ketiga akan dinyahaktifkan sekiranya tidak diakses selama tiga (3) bulan berturut-turut dan ID akan dipadamkan pada bulan berikutnya.</p> <p>c. Borang Permohonan Penamatan VPN Jabatan Akauntan Negara Malaysia adalah seperti di Lampiran 2.</p>	<ul style="list-style-type: none">• Warga JANM• Pihak ketiga



Bil.	Perkara	Peranan
	d. Bagi id VPN (bertempoh) akan ditamatkan serta merta selepas situasi kritikal telah tamat.	
5.	<u>Perlindungan Rangkaian Daripada Perisian Berbahaya</u> a. Mengimbas semua kandungan storan luaran dengan perisian antivirus. b. Memastikan tiada sambungan perkakasan yang mencurigakan pada port <i>Universal Serial Bus</i> (USB) komputer yang disediakan oleh JANM.	<ul style="list-style-type: none">• Warga JANM• Pihak ketiga
6.	<u>Windows Encryption Technology</u> a. Komputer riba yang dibekalkan perlu dipasang dengan <i>windows encryption</i> untuk menghalang dari akses yang tidak dibenarkan bagi melindungi data dan maklumat JANM. b. Memastikan <i>Windows Encryption</i> adalah terkini.	<ul style="list-style-type: none">• Warga JANM
7.	Perkara-perkara berikut adalah <u>TIDAK DIBENARKAN:</u> a. Penggunaan peralatan rangkaian persendirian yang dihubungkan dengan rangkaian JANM tanpa kebenaran.	<ul style="list-style-type: none">• Warga JANM• Pihak ketiga
8.	Keselamatan Rangkaian dan Sistem ICT mesti dilaksanakan mengikut Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang berkuatkuasa.	<ul style="list-style-type: none">• Warga JANM• Pihak ketiga



PERKAKASAN DAN PERISIAN



8.0 PERKAKASAN DAN PERISIAN

Bil.	Perkara	Peranan
1.	<ol style="list-style-type: none">Komputer riba mestilah dikunci dengan <i>cable lock</i> yang dibekalkan atau disimpan dalam kabinet berkunci.Pengguna digalakkan membuat salinan atau penduaan (<i>backup</i>) pada maklumat yang disimpan dalam perkakasan bagi tujuan keselamatan dan bagi mengelakkan kehilangan data. Maklumat yang disimpan adalah mengikut prosedur <i>backup</i> yang telah ditetapkan.	<ul style="list-style-type: none">Warga JANM
2.	<p>Perkara-perkara berikut adalah <u>TIDAK DIBENARKAN</u>:</p> <ol style="list-style-type: none">Meninggalkan cetakan yang mengandungi maklumat Terhad atau Sulit di mesin pencetak atau penyalin atau ditinggalkan di mana-mana lokasi yang terdedah dan tidak selamat;Meletakkan atau menyimpan sebarang maklumat rahsia rasmi di skrin <i>desktop</i> komputer atau komputer riba;Membuat penambahan, menanggal atau mengganti perkakasan ICT yang telah ditetapkan;Mengubah kedudukan perkakasan dari tempat asal kecuali telah mendapat kebenaran Pengurus ICT dan dimaklumkan kepada Pegawai Aset;Menampal sebarang pekat atau melakukan sebarang instalasi dan modifikasi pada perkakasan dan perisian selain untuk tujuan rasmi kecuali mendapat kebenaran Pentadbir ICT dan dimaklumkan kepada Pegawai Aset; danSekiranya pegawai bertukar tempat bertugas ke pejabat atau lokasi yang baharu, pegawai tidak dibenarkan untuk membawa perkakasan ICT dan mesti dikembalikan mengikut tatacara atau prosedur yang ditetapkan.	<ul style="list-style-type: none">Warga JANM



PERKHIDMATAN PRASARANA KUNCI AWAM



9.0 PENGURUSAN KESELAMATAN SISTEM APLIKASI

Bil.	Perkara	Peranan
Pembangunan Sistem		
1.	Menyediakan dokumen pembangunan sistem berdasarkan garis panduan Kejuruteraan Sistem Aplikasi Sektor Awam (KRISA) atau Pengurusan Projek ICT Sektor Awam (PPRISA) atau prosedur dalaman JANM.	<ul style="list-style-type: none">• Pemilik Sistem• Pentadbir Sistem ICT
2.	Menentukan dan mengesahkan peranan dan tahap capaian penggunaan sistem.	<ul style="list-style-type: none">• Pemilik Sistem• Pentadbir Sistem ICT• Penyelaras ICT
3.	Membuat dan mengemaskini konfigurasi peranan dan tahap capaian pengguna sistem.	<ul style="list-style-type: none">• Pentadbir Sistem ICT
4.	Maklumat kata laluan pengguna disimpan dalam bentuk <i>encrypted</i> di dalam pangkalan data.	<ul style="list-style-type: none">• Pentadbir Sistem ICT
5.	Memastikan perlindungan ke atas data terperingkat menggunakan <i>Secure Sockets Layer (SSL)</i> , <i>Secure Shell (SSH)</i> , <i>Public Key Infrastructure (PKI)</i> atau <i>Encryption</i> .	<ul style="list-style-type: none">• Pentadbir Sistem ICT• Penyelaras ICT
6.	Memastikan sistem mempunyai <i>session termination (frontend/backend)</i> .	<ul style="list-style-type: none">• Pentadbir Sistem ICT• Penyelaras ICT
7.	Menyekat paparan <i>Directory Listing</i> .	<ul style="list-style-type: none">• Pentadbir Sistem ICT
8.	Mengkhususkan satu <i>drive/volume/directory</i> secara berasingan untuk Sistem Pengoperasian (OS), Pangkalan Data (DB) dan Aplikasi mengikut kesesuaian dan keperluan.	<ul style="list-style-type: none">• Pentadbir Sistem ICT



**GARIS PANDUAN TEKNOLOGI MAKLUMAT
DAN KOMUNIKASI**

Versi : 1.1

Tahun : 2024

Bil.	Perkara	Peranan
9.	Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang berkuatkuasa mesti dipatuhi untuk mengelak pencerobohan data dan sistem.	<ul style="list-style-type: none">• Pemilik sistem• Pentadbir Sistem ICT
10.	Mesej ralat tidak boleh memaparkan mesej dalaman sistem seperti nama <i>table</i> , <i>prosedur</i> , <i>error code</i> dan sebagainya kepada pengguna bagi mengelakkan risiko digodam.	<ul style="list-style-type: none">• Pentadbir Sistem ICT
11.	URL query string tidak boleh memaparkan sebarang maklumat session pengguna seperti: https://www.example.net/servlet/login?userid=abu&password=abu	<ul style="list-style-type: none">• Pentadbir Sistem ICT
12.	Sistem aplikasi mestilah berupaya menyemak dan memastikan data input yang dimasukkan betul bagi menjamin ketepatan dan integriti maklumat.	<ul style="list-style-type: none">• Pentadbir Sistem ICT
13.	Memastikan ketersediaan sistem dengan menyediakan persekitaran <i>High Availability</i> (jika berkaitan).	<ul style="list-style-type: none">• Pentadbir Sistem ICT• Penyelaras ICT
14.	Memastikan dokumentasi sistem, prosedur operasi standard sistem (<i>Standard Operating Procedure – SOP</i>), dan manual panduan pengguna yang lengkap serta terkini.	<ul style="list-style-type: none">• Pemilik Sistem• Pentadbir Sistem ICT
15.	Memastikan dengan jelas kriteria dan keperluan bagi penerimaan sistem, didokumenkan dan diuji sebelum sistem diterima.	<ul style="list-style-type: none">• Pemilik Sistem• Pentadbir Sistem ICT
16.	Membuat konfigurasi dan pelarasan terhadap sistem pengoperasian, perisian pembangunan sistem dan pangkalan data untuk memberi perlindungan kepada sistem yang akan digunakan supaya keselamatan dan prestasi sistem di tahap yang optimum.	<ul style="list-style-type: none">• Pentadbir Sistem ICT



Bil.	Perkara	Peranan
17.	Memastikan sistem mempunyai jejak audit (<i>audit trail</i>) dan mengaktifkan fail log.	<ul style="list-style-type: none">• Pentadbir Sistem ICT
18.	Melaksanakan aktiviti <i>Security Posture Assessment</i> (SPA) dan pengukuhan sebelum sistem <i>Go Live</i> mengikut Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam.	<ul style="list-style-type: none">• Pentadbir Sistem ICT
19.	Melakukan pengujian iaitu <i>functional</i> , <i>non-functional</i> termasuk <i>stress test</i> dan <i>performance testing</i> untuk <i>validate and verify</i> sistem yang dibangunkan bagi memenuhi keperluan dan rekabentuk sistem.	<ul style="list-style-type: none">• Pemilik Sistem• Pentadbir Sistem ICT• Penyelaras ICT
20.	Pengujian sistem hendaklah dilaksanakan di persekitaran pengujian (<i>Development/Staging</i>) terlebih dahulu bagi meminimakan risiko dan gangguan kepada operasi sistem di <i>Production</i> .	<ul style="list-style-type: none">• Pemilik Sistem• Pentadbir Sistem ICT• Penyelaras ICT
21.	Melakukan pengujian sistem setiap kali selepas proses <i>restore</i> dijalankan.	<ul style="list-style-type: none">• Pemilik Sistem• Pentadbir Sistem ICT
Pengoperasian, Penyenggaraan dan Pemantauan Sistem		
1.	Memastikan sistem mempunyai khidmat sokongan dan penyenggaraan.	<ul style="list-style-type: none">• Pemilik Sistem
2.	Penyenggaraan sistem hanya boleh dilakukan oleh kakitangan atau pihak yang dibenarkan sahaja. Semua aktiviti penyenggaraan hendaklah disemak dan diuji sebelum dan selepas aktiviti tersebut dilaksanakan.	<ul style="list-style-type: none">• Pentadbir Sistem ICT• Pihak Ketiga



Bil.	Perkara	Peranan
3.	Sebarang penyenggaraan yang memerlukan sistem ditutup (<i>shutdown</i>) dan tidak boleh dicapai dalam tempoh tertentu perlu dirancang, dipersetujui dan dimaklumkan kepada pengguna.	<ul style="list-style-type: none">• Pentadbir Sistem ICT• Penyelaras ICT• Pihak Ketiga• Pengguna
4.	Mengurus dan memantau aktiviti penyenggaraan sistem mengikut jadual yang telah ditetapkan.	<ul style="list-style-type: none">• Pemilik Sistem• Pentadbir Sistem ICT• Penyelaras ICT• Pihak Ketiga
5.	Melaporkan sebarang insiden keselamatan berkaitan sistem ke pihak yang bertanggungjawab.	<ul style="list-style-type: none">• Pentadbir sistem ICT• Pemilik sistem
6.	Memastikan dan memantau sistem boleh dicapai dan digunakan pada setiap masa.	<ul style="list-style-type: none">• Pemilik sistem• Pentadbir sistem ICT• Penyelaras ICT
7.	Melaksanakan aktiviti <i>Security Posture Assessment</i> (SPA) dan pengukuhan mengikut Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam.	<ul style="list-style-type: none">• Pentadbir sistem ICT• Penyelaras ICT• Pemilik sistem
8.	Memastikan setiap masalah aplikasi diselesaikan di dalam tempoh <i>Service Level Agreement</i> (SLA) yang ditetapkan di dalam kontrak atau Surat Setuju Terima (SST).	<ul style="list-style-type: none">• Pemilik Sistem• Pihak Ketiga



Bil.	Perkara	Peranan
9.	Bagi sebarang perubahan sistem yang dibuat hendaklah mengikut tatacara proses yang dinyatakan di KRISA atau PPrISA atau Prosedur Kawalan Perubahan.	<ul style="list-style-type: none">• Pemilik• Pentadbir sistem ICT• Penyelaras ICT
10.	Merekod dan menyimpan dokumentasi pembangunan sistem termasuk <i>source code</i> selepas <i>project hand-over</i> dilaksanakan.	<ul style="list-style-type: none">• Pemilik sistem• Pentadbir sistem ICT• Penyelaras ICT
<i>Source Code</i>		
1.	<i>Source code</i> atau <i>Intellectual Property Right (IPR)</i> bagi pembangunan sistem aplikasi dan serahan-serahan lain menjadi hak milik JANM kecuali <i>source code</i> yang telah dipatenkan oleh pihak prinsipal (<i>commercial of the shelf</i>).	<ul style="list-style-type: none">• Pemilik sistem• Penyelaras ICT
2.	Sekiranya terdapat penambahbaikan yang baharu (<i>change request</i>) pada sistem, <i>source code</i> perlu dikemaskini dan disimpan mengikut keperluan JANM.	<ul style="list-style-type: none">• Pentadbir sistem ICT• Pihak Ketiga
3.	Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut: <ul style="list-style-type: none">i. Log audit perlu dikekalkan kepada semua akses kepada kod sumber; danii. Penyelenggaraan dan pinyaliran kod sumber hendaklah tertakluk kepada kawalan perubahan.	<ul style="list-style-type: none">• Pentadbir sistem• Pemilik sistem• Pihak ketiga



10.0 PERKHIDMATAN PRASARANA KUNCI AWAM – GOVERNMENT PUBLIC KEY INFRASTRUCTURE (GPKI)

Bil.	Perkara	Peranan
1.	Pentadbir GPKI perlu dilantik bagi mengurus sijil digital pengguna.	<ul style="list-style-type: none">• Pentadbir GPKI
2.	Permohonan pembaharuan, pembatalan dan semakan status sijil digital pengguna hendaklah melalui portal atau <i>mobile</i> GPKI.	<ul style="list-style-type: none">• Pentadbir dan Pengguna GPKI
3.	Pemegang sijil digital perlu mematuhi Garis Panduan dan merujuk Portal MyGPKI Jabatan Digital Negara yang dikemaskini dari semasa ke semasa.	<ul style="list-style-type: none">• Pentadbir dan Pengguna GPKI
4.	Pemegang sijil digital perlu memaklumkan kepada pentadbir GPKI berkenaan penggantian dan pembatalan sijil digital pengguna mengikut keperluan berikut: <ul style="list-style-type: none">a. Sijil digital yang tidak berfungsi;b. Sijil digital yang disalahguna oleh pihak ketiga;c. Penyalahgunaan oleh pemegang sijil digital pengguna; dand. Pengguna yang tamat perkhidmatan atau bersara.	<ul style="list-style-type: none">• Pentadbir dan Pengguna GPKI



PIHAK KETIGA



11.0 PIHAK KETIGA

Bil.	Perkara	Peranan
1.	<p>Pihak ketiga yang dilantik yang memerlukan akaun bagi mendapat capaian ke sistem-sistem di JANM perlu melengkapkan dokumen seperti di bawah:</p> <ol style="list-style-type: none">Salinan borang permohonan ke sistem e-Vetting, Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) - https://evetting.cgso.gov.my;Surat Akaun Pematuhan Polisi Keselamatan Siber JANM (rujuk PKS versi terkini);Borang Permohonan Pendaftaran VPN Jabatan Akauntan Negara Malaysia – jika perlu;Borang Perakuan Untuk Ditandatangani Oleh Komuniti Keselamatan Atau Mana-Mana Pihak Lain yang Berurusan Dengan Perkhidmatan Awam Atau Yang Berkhidmat di Kediaman Rasmi Kerajaan Berkaitan Dengan Akta Rahsia Rasmi 1972 [Akta 88] seperti di Lampiran 3; danBorang Perakuan Untuk Ditandatangani oleh Komuniti Keselamatan Atau Mana-Mana Pihak Lain yang Berurusan Dengan Perkhidmatan Awam atau Yang Berkhidmat di Kediaman Rasmi Kerajaan Apabila Tamat Kontrak Perkhidmatan Dengan Kerajaan Berkaitan dengan Akta Rahsia Rasmi 1972 [Akta 88] seperti di Lampiran 4 (untuk penamatan pembekal).	<ul style="list-style-type: none">Pihak ketigaPentadbir Sistem
2.	<p>Pentadbir sistem bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pihak ketiga.</p>	<ul style="list-style-type: none">Pentadbir ICT
3.	<p>Pihak ketiga hendaklah menyerahkan kod sumber (<i>source code</i>) sistem enam (6) bulan sebelum kontrak tamat kepada pihak JANM.</p>	<ul style="list-style-type: none">Pihak ketigaPemilik Sistem



**GARIS PANDUAN TEKNOLOGI MAKLUMAT
DAN KOMUNIKASI**

Versi : 1.1


Tahun : 2024

Bil.	Perkara	Peranan
4.	Penilaian prestasi pihak ketiga perlu dilaksanakan secara berkala dan mengikut keperluan.	<ul style="list-style-type: none">• Pihak ketiga• Pemilik Sistem

12.0 GLOSARI

TERMA	PENERANGAN
BPTM	Bahagian Pengurusan Teknologi Maklumat
PKS	Polisi Keselamatan Siber
GPKI	<i>Government Public Key Infrastructure</i>
iGFMAS	<i>integrated Government Financial and Management Accounting System</i>
ISO/IEC27001:2022	<i>International Standard 27001:2022 – Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements</i>
JANM	Jabatan Akauntan Negara Malaysia
KRISA	Kejuruteraan Sistem Aplikasi Sektor Awam (KRISA)
PPriSA	Pengurusan Projek ICT Sektor Awam (PPriSA)
RAKKSSA	Rangka Kerja Keselamatan Siber Sektor Awam
SOP	<i>Standard Operating Procedure</i>
SSID	<i>Service Set Identifier</i>
USB	<i>Universal Serial Bus</i>
VPN	<i>Virtual Private Network</i>

Borang Permohonan *Virtual Private Network (VPN)*
Jabatan Akauntan Negara Malaysia

	BORANG PERMOHONAN VIRTUAL PRIVATE NETWORK (VPN) JABATAN AKAUNTAN NEGARA MALAYSIA	VPN Kakitangan Kerajaan <input type="checkbox"/> VPN Bertempoh <input type="checkbox"/> VPN Pihak Ketiga <input type="checkbox"/>
---	---	---

Kepada: Pengarah Bahagian Pengurusan Teknologi Maklumat

BIL	PERKARA	MAKLUMAT
1.	Nama Pemohon* (Huruf Besar)	
2.	Jawatan*	
3.	Nombor Kad Pengenalan / <i>Passport</i> *	
4.	Warganegara*	
5.	Alamat E-mel Rasmi*	
6.	No. Telefon*	
7.	Nama Organisasi*	
8.	Alamat Organisasi*	
9.	Nyatakan tahap dan justifikasi keperluan akses ke sistem-sistem tertentu di JANM (jika ada): Lokasi Sistem: <input type="checkbox"/> HO (Ibu Pejabat JANM) <input type="checkbox"/> PRD (I-City, Shah Alam) <input type="checkbox"/> DRC (Petaling Jaya) <input type="checkbox"/> Pejabat Perakaunan (Nyatakan) : <div style="border: 1px solid black; width: 150px; height: 20px; margin-left: 20px;"></div>	Maklumat yang diperlukan: a) No. Siri PC* : b) Physical Address* : Start > cmd (enter) > ipconfig /all (enter) Senarai IP Address Server/Sistem yang hendak diakses: a) _____ b) _____

***wajib diisi**

Pengakuan Pemohon:

Saya akan mematuhi segala peraturan yang termaktub dalam Akta Rahsia Rasmi 1972, Akta Jenayah Komputer 1997, Akta Komunikasi dan Multimedia 1998 serta semua pekeliling dan peruntukan berkaitan dengan perlindungan maklumat dan rahsia Kerajaan Malaysia. Saya juga akan memaklumkan kepada pihak Bahagian Pengurusan Teknologi Maklumat, JANM mengenai penamatan perkhidmatan saya sebagai kakitangan organisasi yang tersebut diatas atau apabila kontrak organisasi dengan JANM tamat dengan mengisi dan menghantar Borang Permohonan Penamatan *Virtual Private Network (VPN)* JANM. Saya juga bersetuju:

- VPN Kakitangan Kerajaan:** ID VPN saya akan ditamatkan secara automatik setelah enam (6) bulan tidak akses.
- VPN Bertempoh:** ID VPN saya akan ditamatkan secara automatik setelah kecelakaan/bencana tamat.
- VPN Pihak Ketiga:** ID VPN saya akan ditamatkan secara automatik setelah tiga (3) bulan tidak akses.

Tandatangan Pemohon & Nama Penuh*:

.....

Tarikh :

Pengesahan Ketua Unit/Seksyen & Cop Rasmi*:

.....

Tarikh :

Maklumat Permohonan: Untuk Kegunaan BPTM sahaja

Dimaklumkan bahawa permohonan anda telah diluluskan.

Berikut adalah maklumat akaun *Virtual Private Network* (VPN) anda:

Nama Sistem	Pengesahan Pentadbir Sistem		ID/Username	Catatan
	Nama	Tandatangan		

Sebarang pertanyaan mengenai perkara ini hendaklah berurusan terus dengan:


**Unit Pengurusan Rangkaian dan Keselamatan,
 Aras 5, Bahagian Pengurusan Teknologi Maklumat,
 Kompleks Kementerian Kewangan,
 No. 1, Persiaran Perdana, Presint 2,
 62594 Putrajaya.**

Tel : 03-8882 1232 / 03-8882 1266

Emel : networksecurity@anm.gov.my

*Sila tandakan " / " pada kotak berkenaan.

**Borang Permohonan Penamatan *Virtual Private Network (VPN)*
Jabatan Akauntan Negara Malaysia**

		BORANG PERMOHONAN PENAMATAN VIRTUAL PRIVATE NETWORK (VPN) JABATAN AKAUNTAN NEGARA MALAYSIA		VPN Kakitangan Kerajaan <input type="checkbox"/> VPN Bertempoh <input type="checkbox"/> VPN Pihak Ketiga <input type="checkbox"/>
Kepada: Pengarah Bahagian Pengurusan Teknologi Maklumat				
BIL	PERKARA	MAKLUMAT		
1.	Nama Pemohon* (Huruf Besar)			
2.	Jawatan*			
3.	Nombor Kad Pengenalan / <i>Passport</i> *			
4.	Warganegara*			
5.	Alamat E-mel Rasmi*			
6.	No. Telefon*			
7.	Nama Organisasi*			
8.	Alamat Organisasi*			
9.	Sebab-Sebab penamatan	<input type="checkbox"/> 9.1 Tugas di JANM selesai / ditamatkan oleh syarikat pembekal / Organisasi / JANM <input type="checkbox"/> 9.2 Bersara / Tamat Perkhidmatan di syarikat pembekal / Organisasi / JANM <input type="checkbox"/> 9.3 Melanggar prosedur penggunaan tempat / sistem di JANM (sila nyatakan) <input type="checkbox"/> 9.4 Lain-lain (sila nyatakan)		
Nota: Bagi perkara 9.3, borang ini perlulah ditandatangani oleh Timbalan Pengarah, Seksyen Perkhidmatan ICT BPTM. Dengan ini adalah disahkan akaun <i>Virtual Private Network (VPN)</i> pengguna berkenaan ditamatkan atas sebab-sebab di atas.				
Tandatangan Wakil Organisasi: Tarikh:			Pengesahan Ketua Unit/Seksyen & Cop Rasmi: Tarikh:	

Maklumat Permohonan:

Maklumat Permohonan: Untuk Kegunaan BPTM sahaja

Dimaklumkan bahawa permohonan penamatan ini telah diambil tindakan.

Berikut adalah maklumat akaun *Virtual Private Network (VPN)* yang telah ditamatkan:

Nama Sistem	Pengesahan Pentadbir Sistem		ID/Username	Tarikh Penamatan Akses
	Nama	Tandatangan		

Sebarang pertanyaan mengenai perkara ini hendaklah berurusan terus dengan:

**Unit Pengurusan Rangkaian dan Keselamatan,
Aras 5, Bahagian Pengurusan Teknologi Maklumat,
Kompleks Kementerian Kewangan,
No. 1, Persiaran Perdana, Presint 2,
62594 Putrajaya.**

Tel : 03-8882 1232 / 03-8882 1266

Emel : networksecurity@anm.gov.my

**Borang Perakuan Untuk Ditandatangani Oleh Komuniti Keselamatan Atau Mana-
Mana Pihak Lain yang Berurusan Dengan Perkhidmatan Awam Atau Yang
Berkhidmat di Kediaman Rasmi Kerajaan Berkaitan Dengan Akta Rahsia Rasmi 1972
[Akta 88]**

**PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN
ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN
PERKHIDMATAN AWAM ATAU YANG BERKHIDMAT DI KEDIAMAN RASMI
KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]**

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan surat rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Saya faham bahawa segala rahsia rasmi dan surat rasmi yang saya peroleh semasa berurusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan atau menyampaikan, sama ada secara lisan, bertulis atau dengan cara elektronik kepada sesiapa jua dalam apa-apa bentuk, sama ada dalam masa atau selepas berurusan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapatkan kebenaran bertulis daripada pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani satu akuan selanjutnya bagi maksud ini apabila urusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia telah selesai.

Tandatangan	:
Nama (huruf besar)	:
No. Kad Pengenalan	:
Jawatan	:
Jabatan / Organisasi	:
Tarikh	:
Disaksikan oleh	:
	 (Tandatangan)
Nama (huruf besar)	:
No. Kad Pengenalan	:
Jawatan	:
Jabatan / Organisasi	:
Tarikh	:
Cap Jabatan / Organisasi	:

Borang Perakuan Untuk Ditandatangani oleh Komuniti Keselamatan Atau Mana-Mana Pihak Lain yang Berurusan Dengan Perkhidmatan Awam atau Yang Berkhidmat di Kediaman Rasmi Kerajaan Apabila Tamat Kontrak Perkhidmatan Dengan Kerajaan Berkaitan dengan Akta Rahsia Rasmi 1972 [Akta 88]

PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN PERKHIDMATAN AWAM ATAU YANG BERKHIDMAT DI KEDIAMAN RASMI KERAJAAN APABILA TAMAT KONTRAK PERKHIDMATAN DENGAN KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan surat rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Dengan ini menjadi satu kesalahan di bawah Akta tersebut bagi saya menyampaikan dengan tiada kebenaran apa-apa rahsia rasmi atau surat rasmi kepada mana-mana orang lain, sama ada atau tidak orang itu memegang jawatan dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau mana-mana Kerajaan Malaysia, dan sama ada di Malaysia atau di negara luar, sebelum dan selepas saya tamat kontrak perkhidmatan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia.

Saya mengaku bahawa tidak lagi ada dalam milik saya atau kawalan saya apa-apa perkataan kod rasmi, isyarat timbal, atau kata laluan rasmi yang rahsia, atau apa-apa benda, surat atau maklumat, anak kunci, lencana, alat meteri, atau cap bagi atau yang dipunyai, atau diguna, dibuat atau diadakan oleh mana-mana jabatan Kerajaan atau oleh mana-mana pihak berkuasa diplomat yang dilantik oleh atau yang bertindak di bawah kuasa Kerajaan Malaysia atau Seri Paduka Baginda Yang di-Pertuan Agong yang tidak dibenarkan berada dalam milikan atau kawalan saya.

Tandatangan :
 Nama (huruf besar) :
 No. Kad Pengenalan/ Pasport :
 Jawatan :
 Jabatan/Organisasi :
 Tarikh :
 Disaksikan oleh :
 (Tandatangan)
 Nama (huruf besar) :
 No. Kad Pengenalan/ Pasport :
 Jawatan :
 Jabatan/Organisasi :
 Tarikh :
 Cap Jabatan / Organisasi :